



## netfence Management Centres

### Secure Connectivity zentral verwaltet

Sicherheitsbewusste Unternehmen und Managed Security Provider sehen sich mit einer rasant steigenden Zahl von Gateways in ihren Netzwerken konfrontiert. Diese Gateways müssen ausgerollt, konfiguriert und permanent überwacht werden. Unabhängig davon, wie komfortabel die Installation und die laufende Pflege eines einzelnen Gateways ist, hunderte oder tausende Systeme einzeln zu administrieren erfordert einen enormen Einsatz von qualifiziertem Personal und ist kostenintensiv.

Gleichzeitig muss eine unternehmensweite Security Policy ständig auf allen Gateways gepflegt werden. Dadurch werden die Konfigurationen einzelner Systeme immer mehr miteinander verschränkt. Schon ein einfacher Site-to-Site VPN-Tunnel setzt voraus, dass mindestens zwei Gateways aufeinander abgestimmt sind. In großen Umgebungen mit hunderten solcher Installationen bedeutet das, dass die Kosten für Konfiguration und Betrieb nicht proportional zur Anzahl der Systeme sondern exponentiell ansteigen.

netfence Management Centres sind Software-basierte dedizierte Server zum Management von netfence gateways und phionOS basierten Servern. Dadurch wird die herausragende GUI-Managebar-

keit einzelner netfence gateways um eine zentralisierte Administrationskomponente erweitert.

netfence Management Centres ermöglichen es, die Kosten für den Betrieb erheblich zu senken und erweitern gleichzeitig die Funktionalität der Gateways. Darüber hinaus verhindern netfence Management Centres, dass Widersprüche in der Security Policy übersehen werden.

Administratoren bekommen mit netfence Management Centres jederzeit den vollen Überblick über alle Vorgänge auf den gemanagten Gateways und deren Zustand in Echtzeit, können Konfiguration und Software updaten, aber auch Berechtigungen und Rollen global definieren. Die Langzeitstatistik schafft den Überblick über alle historischen Aktivitäten auf den Gateways und liefert die Daten für die Planung, Kontrolle und Verrechnung der Kosten von Konnektivität.

Das zentrale Management mit netfence Management Centres dient nicht nur zur Konfiguration und Administration der netfence gateways. Die in einer zentralen Datenbank gespeicherten Konfigurations- und Lizenzdaten ermöglichen ein Disaster Recovery in weniger als 4 Minuten. Das ist nur möglich, da keine neuen Lizenzdaten angefordert werden müssen und die Konfiguration eines Gateways aus dem zentralen Datenbestand vollständig reproduziert

### Features & Benefits

#### ➤ Zentrales Management für Firewall und VPN Policy

Umfassendes Zentrales Management spart Kosten und erhöht die Sicherheit.

#### ➤ Visualisierung

Informieren Sie sich mit nur einem Blick über den Zustand aller Ihrer netfence gateways.

#### ➤ VPN GTI

Erstellen Sie mit Drag&Drop im Graphical Tunnel Interface VPN Standortvernetzungen. Konfigurieren Sie global Parameter und nutzen Sie die Möglichkeit des Übersteuerns für jeden einzelnen Tunnel.

#### ➤ Skalierbarkeit

Garantiert die netzwerkübergreifende Durchgängigkeit von Sicherheitsstrategien, unabhängig von der Größe des Netzwerks - von wenigen bis zu mehreren hundert netfence gateways und Appliances.

#### ➤ Full Service Remote System Management

Management umfasst alle Systemeinstellungen der Gateways. Erleben Sie Remote Software Updates, die auch wirklich funktionieren.

#### ➤ Hervorragender TCO

Starkes rollenbasierendes Administrationsmodell zur sicheren Delegation von Administrationsaufgaben. Damit erhöhen Sie gleichzeitig Effizienz und Sicherheit der Administration.

#### ➤ Volle Auditierbarkeit dank RCS-Integration

Durch vollintegriertes Revision Control System sind alle verwalteten netfence gateways schnell und einfach auditierbar.

#### ➤ Public Key Infrastructure

phion PKI für Erstellung und Verwaltung von digitalen x.509v3 Zertifikaten.

# netfence Management Centres

werden kann.

netfence Management Centres gibt es in drei Produktvarianten:

- **Management Centre Entry** wurde für kleinere Unternehmen mit weniger als 50 Devices entwickelt.
- **Management Centre Enterprise** ist die Lösung für mittlere und große Unternehmen, in denen die Delegation und Nachvollziehbarkeit von administrativen Aufgaben eine Voraussetzung ist. Management Centre Enterprise bietet die Möglichkeit, netfence gateways in organisatorische Gruppen zusammenzufassen. Neue Gateways, die der Gruppe hinzugefügt werden, bekommen automatisch die entsprechenden Konfigurationen und Policies zugewiesen.
- **Management Centre Global Player** ist die ideale Lösung für große Unternehmen oder Managed Security Provider mit großen Security Umgebungen, die bis zu mehrere hundert Gateways umfassen. Das hierarchische, 2-stufige Management beruht auf Servergruppen und sog. Ranges. Ein Range besteht aus mehreren Servergruppen, die entweder die Systeme eines Kunden oder einen Teil des Netzwerkes eines großen Unternehmens darstellen.

## Umfassende Administration

netfence Management Centres gehören zu den umfassendsten und flexibelsten Managementinstrumenten auf dem Markt und passen sich ideal und einfach an die Bedürfnisse großer Umgebungen mit vielen Installationen oder weltweit verteiltem Personal an. Das hierarchische Management gruppiert alle gemanagten Gateways in Servergruppen, die wiederum in Ranges eingeteilt werden.

Administratoren können ein oder mehrere Domains besitzen, die aus Ranges und/oder Servergruppen bestehen. In jedem dieser Zuständigkeitsbereiche können einem Administratoren unterschiedliche frei definierbare Rollen zugewiesen werden. Die Rollenprofile werden zentral festgelegt und bestimmen die jeweiligen Konfigurationsrechte, die Monitoring Optionen und welche Reports eingesehen werden können. Diese Einstellungen gelten sowohl im Management Centre, als auch auf den Gateways im jeweiligen Zuständigkeitsbereich. Übergeordnete Administratoren behalten aber jederzeit den vollen Zugriff auf die Gateways.

Die ausgeprägte Multiadministrator-Fähigkeit ermöglicht, dass dieselben Rechte an mehrere Administratoren vergeben werden. Dadurch wird konsequentes 7x24 Management selbst größter und geografisch verteilter Netzwerke möglich.

## Konfigurationsmanagement

netfence Management Centre Series bieten alle Managementfunktionalitäten, um Unternehmen eine kostengünstige Installation und Administration selbst größter IT-Infrastrukturen zu ermöglichen. Das

zentralisierte Konfigurationsmanagement ist GUI-basiert und verwaltet alle Konfigurationsdaten und Einstellungen des Betriebssystems, sowie Firewall-Regelsätze und VPN-Policies. Das Konfigurationsmanagement ist session- und transaktionsbasiert, verwendet exklusive Data locks für gerade bearbeitete Daten und bleibt so multiadministratorentauglich.

Damit alle Gateways dieselben Konfigurationen und Security Policies verwenden, besitzen die Management Centre Series ein zentrales Repository. So werden alle Gateways, die auf dieselben Konfigurationsfiles zugreifen nach der Änderung automatisch aktualisiert.

Zentralisierte Konfiguration bringt aber auch mehr Flexibilität in hoch verfügbare Systeme und unterstützt Load Balancing.

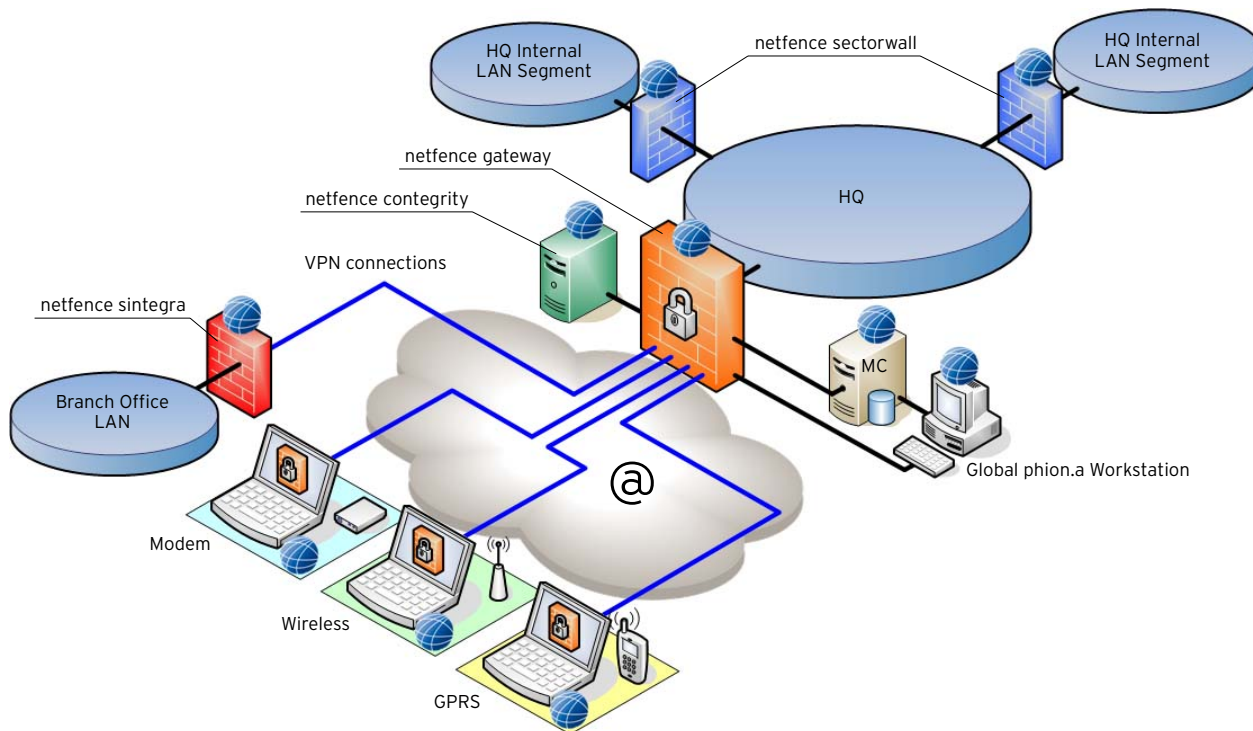
Das Konzept eines aktiven und eines ungenutzten Hot-Standby Gateways wird durch ein Konzept ersetzt, das ein primäres und sekundäres Gateway für einen bestimmten Service vorsieht. Dadurch kann ein Gateway primär für Firewall und VPN zuständig sein und sekundär als HTTP-Proxy und SMTP Mail Gateway verwendet werden. Auf diese Art und Weise sind beide Gateways im Einsatz und sind gleichzeitig zueinander hochverfügbar. Dieses Hochverfügbarkeitskonzept kann sehr einfach auf drei oder mehr Gateways erweitert werden, wodurch wiederum Lizenz- und Hardwarekosten eingespart werden können. Die Sicht des Administrators auf die Konfigurationsstruktur ist an die Erfordernisse des Aufgabengebiets angepasst. Als zusätzliche Sicherheitsmaßnahme kann jedem Administrator ein eigener Konfigurationsparameter zugewiesen werden, der die Modifikation von bestimmten Konfigurationen verbietet und sogar bestimmte Konfigurationsdateien innerhalb seiner eingeschränkten Ansicht ausblendet.

## Monitoring und Reporting

Große Netzwerktopologien befinden sich ständig in Bewegung. netfence Gateways überwachen diese Vielzahl von Vorgängen, Aktionen und Veränderungen und reporten diese an das Management Centre. Damit ist der Administrator sofort über Netzwerkattacken, den Ausfall von Leitungen oder Routen, den Systemzustand oder über operative Probleme informiert. Mit der Management Centre Status Map wird ein übersichtlicher Echtzeit-Gateway-Status auf einen Blick ermöglicht. Vom Gesamtsystem über einzelne Servergruppen bis hin zur Einzelmaschine werden verschiedenste Informationen übersichtlich visualisiert. Darüber hinaus ist die Status Map auch als Launch Pad für den direkten Management Zugang für jedes einzelne im Verbund befindliche Gateway verwendbar. Das ist insbesondere bei Gateways mit dynamischen IP Adressen von Vorteil, bei denen das MC als Tunnel Endpunkt agiert. Der Direktzugriff erfolgt via SSL und nutzt zwischen MC und Gateways eine auf x.509v3 Zertifikaten basierten Trust Chain.

Alle Administratorenzugriffe auf Gateways werden entsprechend geloggt. Ein zentraler Session View listet alle Zugriffe auf Gateway/ Quell IPs, die Art des Zugriffs, den Namen des Administrators sowie

# Zentrales Management für Ihre Sicherheitsinfrastruktur



die Zugriffsdauer auf. Die Informationen, die jedes netfence Gateway an das Management Centre sendet, sind bedarfsgerecht, sowohl in ihrer Häufigkeit, als auch in Zusammensetzung konfigurierbar. Das Management Centre sammelt die Daten aller Gateways und verarbeitet diese zu Gesamt-, Bereichs- oder Gruppenstatistiken.

Das Management Centre ermöglicht aber auch das die Entgegennahme bzw. das gefilterte Relaying von gestreamten Logdaten zu einem externen Security Event Management System.

Alle kritischen System Events werden laufend an das Management Centre berichtet, in eine zentralen Event Liste eingetragen und lösen eine im Management Centre entsprechend konfigurierbare Aktionen aus (SNMP Traps, eMails, etc.).

## VPN Graphical Tunnel Interface (GTI)

Vor allem in sehr komplexen Netzwerkarchitekturen kann das Verwalten von VPN Tunneln eine durchaus schwierige Aufgabe sein. Um das Konfigurieren und Verwalten von VPN Verbindungen komfortabler und einfacher zu gestalten, stellt phion das GTI zur Verfügung. Diese grafische User Interface stellt die VPN Struktur dar und ermöglicht gleichzeitig das Hinzufügen oder Umleiten von VPN Tunneln durch Drag&Drop Funktionalität (gleichgültig ob es sich dabei um eine Hub-spoke oder Fully-meshed VPN Struktur handelt). Die Konfiguration solcher VPN Tunnel-Verbände wird über globale Parameter abgewickelt, die aber in Folge für jeden VPN Tunnel übersteuert werden können, um den individuellen Bedürfnissen gerecht zu werden.

## Remote System Management

Je größer die Anzahl von gemanagten Gateways, desto wichtiger wird der Aufwand für Administration und die Pflege der Infrastruktur. netfence Management Centres sind in der Lage, sowohl Hot Fixes als auch Major Update Prozeduren inklusive phionOS- und Linux-Kernel-Updates zentral abzuwickeln. Updatepakete werden mit wenigen Mouse Klicks an die ausgewählten Gateways transferiert.

Insbesondere für Nicht-Standard-Operationen ist es notwendig, einen direkten Zugriff auf das Betriebssystem zu haben. Deshalb ermöglichen Management Centres eine sichere Remote-Execution-Umgebung (SSHv2) für entsprechend berechnigte Administratoren. So können Kommandos für viele Gateways einfach, sicher und effizient gesendet werden.

## Revision Control System

In modernen Security-Konzepten spielt die Nachvollziehbarkeit und Revisionierbarkeit eine entscheidende Rolle. Die Fähigkeiten des phion RCS' reichen von der Differenz-Anzeige beliebiger Konfigurationsstände der Konfigurationsknoten, über das Erstellen von Reports von Teilen oder der gesamten Konfiguration, bis hin zur Möglichkeit historische Konfigurationen wiederherzustellen. Zusätzlich werden alle Änderungen in der Konfiguration in ein zentrales Logfile geschrieben.

## Public Key Infrastructure

Durch Intregation einer zentralisierten Zertifikatsverwaltung bekommen auch Unternehmen, die über keine eigene PKI verfügen, die Möglichkeit, von den Vorteilen der x.509 Technologie im gesamten netfence-Verband zu profitieren und gegebenenfalls auch Fremdsysteme kostengünstig mit Zertifikaten zu versorgen.

Configuration management	MC Entry	MC Enterprise	MC Global Player
Maximum gateways (recommended, not limited)	50	200	1000+
Configuration templates (repositories)	Yes	Yes	Yes
Shared configuration data	Yes	Yes	Yes
Operating system parameters	Yes	Yes	Yes
Networking/routing parameters	Yes	Yes	Yes
FW/VPN policies, Application gateway parameters	Yes	Yes	Yes
Flat file data storage	Yes	Yes	Yes
Database characteristics (transaction orientation, locking, etc.)	Yes	Yes	Yes
Backup and restore functionality	Yes	Yes	Yes
Gateway configuration archive for speed install	Yes	Yes	Yes
Hierarchy levels	1	2	3
Number of ranges	-	1	5/Optional
Configuration update monitoring	Yes	Yes	Yes
Full RCS versioning	Optional	Optional	Yes
VPN GTI	Yes	Yes	Yes

Status map	MC Entry	MC Enterprise	MC Global Player
Gateway health state	Yes	Yes	Yes
Launch pad functionality	Yes	Yes	Yes
Customisable layout	Yes	Yes	Yes

Trust centre	MC Entry	MC Enterprise	MC Global Player
Gateway x.509 certificate CA (RSA 1024-bit)	Yes	Yes	Yes
Gateway SSH key management (DSA 1024-bit)	Yes	Yes	Yes
SSL-VPN server for tunnels to gateways	Yes	Yes	Yes
Virtual IP addresses for gateways (ProxyARP)	Yes	Yes	Yes
Dynamic gateway IP address support	Yes	Yes	Yes

License centre	MC Entry	MC Enterprise	MC Global Player
License timestamp server	Yes	Yes	Yes
License status display	Yes	Yes	Yes
Central event messagelist	Yes	Yes	Yes
Event forwarding (SNMP, mail)	Yes	Yes	Yes
Event log	Yes	Yes	Yes

Central session tracking	MC Entry	MC Enterprise	MC Global Player
Session display	Yes	Yes	Yes
Session termination	Yes	Yes	Yes

Central software update	MC Entry	MC Enterprise	MC Global Player
Realtime version display	Yes	Yes	Yes
Kernel and OS updates	Yes	Yes	Yes
netfence updates	Yes	Yes	Yes
Update log viewer	Yes	Yes	Yes

Secure remote exec. environment (SSHv2)	MC Entry	MC Enterprise	MC Global Player
Job scheduling	Yes	Yes	Yes
Script management	Yes	Yes	Yes
Execution log viewer	Yes	Yes	Yes

Administration model	MC Entry	MC Enterprise	MC Global Player
Fully phiona GUI based access	Yes	Yes	Yes
Strong authentication and AES encryption	Yes	Yes	Yes
Role-based administration	Yes	Yes	Yes
Configurable roles	Yes	Yes	Yes
Adjustable view on configuration tree	Yes	Yes	Yes
Configurable administrative domains	No	Yes	Yes
Multiple domains per administrator	No	Yes	Yes
Configurable access on OS level	Yes	Yes	Yes
Configurable access notification	Yes	Yes	Yes

Reporting and accounting	MC Entry	MC Enterprise	MC Global Player
Historical reports on gateway activity	Optional	Yes	Yes
Customer based gateway activity reports	Optional	Yes	Yes
Policy distribution	Yes	Yes	Yes
MC-resource utilisation	Yes	Yes	Yes
Gateway-resource utilisation	Optional	Yes	Yes
Central log host	-	Yes	Yes
Streaming/relaying to external log host	Optional	Optional	Yes

Additional functions	MC Entry	MC Enterprise	MC Global Player
NTP4 time server for gateways	Yes	Yes	Yes
Integrated DNS server	Yes	Yes	Yes
High availability	Optional	Optional	Included
e-Security interface	-	Optional	Yes
Public Key Infrastructure	Optional	Yes	Yes
Revision Control System	Optional	Optional	Yes

#### Affiliations & Partnerships

