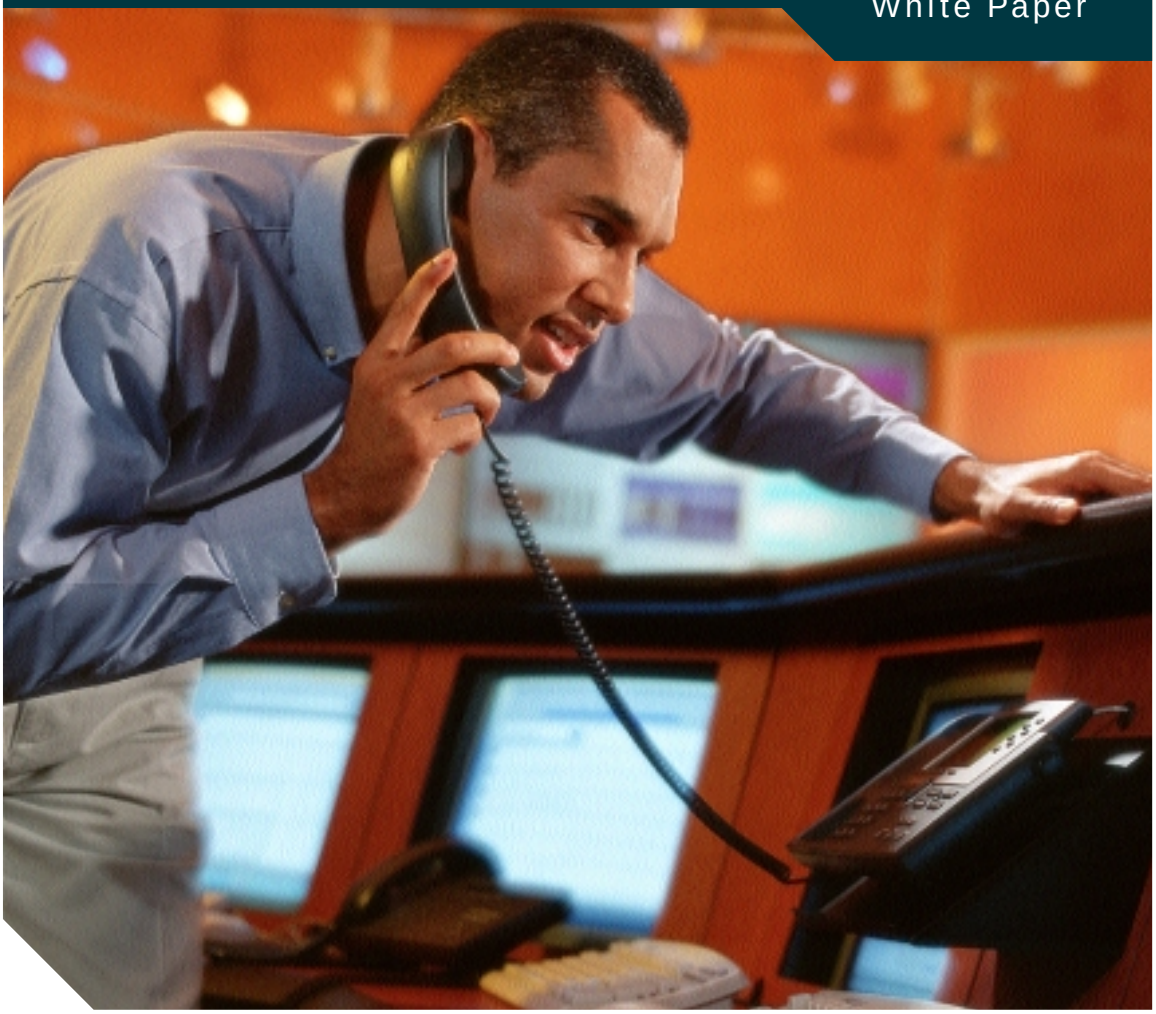
Cisco Systems

White Paper



VPN and Security

Cisco SAFE Security-Konzept für Sicherheit im E-Business

Das vorliegende Dokument bietet allen Interessierten Best-Practice-Informationen für die Gestaltung und Implementierung sicherer Netzwerke. Es soll als Einführung in das SAFE-Konzept dienen und orientiert sich stark am SAFE White Paper für Netzwerke in Klein- und Mittelbetrieben und für dezentrale Nutzer. Das ursprüngliche SAFE White Paper war als Richtlinie für das Sicherheitsdesign von Netzwerken in Großunternehmen gedacht und wird allen empfohlen, die an einer in die Tiefe gehenden technischen Analyse interessiert sind.

Der vorliegende Beitrag setzt die SAFE-Richtlinien in die Anforderungen kleinerer Netzwerke um, z. B. für Zweigstellen großer Unternehmen oder eigenständige Sicherheitsinstallationen in kleinen bis mittelgroßen Unternehmen. Es enthält auch Informationen über Netzwerke für dezentrale Nutzer wie Heimarbeiter und mobile Arbeitskräfte.

SAFE dient als Richtlinie für Netzwerkdesigner, die sich mit der Erfüllung der Sicherheitsanforderungen der Netzwerke beschäftigen müssen. SAFE ist ein in der Tiefe ansetzendes Konzept für die Netzwerksicherheit. Ein solches Sicherheitskonzept orientiert sich an den zu erwartenden Bedrohungen und den Verfahren zu ihrer Minimierung und beschränkt sich nicht auf einfache Anweisungen, an welchen Stellen z. B. eine Firewall oder ein Intrusion-Detection-System einzusetzen ist. Diese Strategie bietet den Vorteil, dass sie eine mehrschichtige Sicherheitsstruktur aufbaut, in der das Versagen eines einzelnen Sicherheitssystems nicht notwendigerweise zu einer Gefährdung der Netzwerkressourcen führt.

Obwohl SAFE unter Verwendung von Produkten von Cisco und dessen Partnern konzipiert wurde, werden die betreffenden Produkte in diesem Dokument nicht explizit genannt. Das heißt, die einzelnen Komponenten werden nicht anhand ihrer Modellnummern, sondern anhand ihrer Funktion identifiziert. Während der Validierungsphase von SAFE wurden echte Produkte exakt in der hier beschriebenen Netzwerk-Implementierung konfiguriert.

Das zentrale Thema im Rahmen dieses Dokumentes sind die Sicherheitsrisiken, denen Netzwerkumgebungen in Unternehmen heute ausgesetzt sind. Netzwerkdesigner, die diese Risiken kennen, können gezielt entscheiden, wo und auf welche Weise sie Abwehrmechanismen einsetzen. Wo dieses Wissen über die Risiken für die Netzwerksicherheit fehlt, besteht die Gefahr, dass Abwehrmechanismen falsch konfiguriert oder zu stark auf die Sicherheitseinrichtungen ausgerichtet werden, oder dass nicht flexibel genug auf die Gefahren reagiert werden kann. Auf der Basis des Konzeptes zur Minimierung solcher Risiken soll das vorliegende Dokument den Netzwerkdesignern die benötigten Informationen liefern, damit sie die richtigen Entscheidungen für die Netzwerksicherheit treffen.

Der nachfolgend durchgängig gebrauchte Begriff “Hacker” bezeichnet eine Person, die in bösartiger Absicht versucht, sich einen unerlaubten Zugang zu Netzwerkressourcen zu verschaffen. Obwohl man eher davon sprechen kann, dass solche Personen versuchen, ein Netzwerk zu “knacken”, soll hier der gebräuchliche Begriff “Hacker” beibehalten werden.

Übersicht über die SAFE-Architektur

Gestaltungsprinzipien

SAFE bildet die funktionalen Anforderungen der heutigen Netzwerke so realitätsgetreu wie möglich nach. Die konkrete Implementierungsentscheidung kann je nach geforderter Netzwerkfunktionalität im Einzelfall verschieden ausfallen. Jedoch können die nachstehend in der Reihenfolge ihrer Bedeutung genannten Gestaltungsziele eine Richtlinie für den Entscheidungsprozess darstellen.

- Sicherheit und Abwehr von Angriffen auf Policy-Basis
- Implementierung von Sicherheit durch die Infrastruktur (und nicht nur durch spezielle Sicherheitseinrichtungen)
- Kostengünstige Realisierung
- Sichere Management- und Reporting-Lösung
- Authentifizierung und Autorisierung von Benutzern und Administratoren für wichtige Netzwerkressourcen
- Erkennung von Angriffen für wichtige Ressourcen und Teilnetze

SAFE ist in erster Linie eine Sicherheitsarchitektur. Sie muss so weit wie möglich verhindern, dass Angriffe auf wertvolle Netzwerkressourcen Erfolg haben. Angriffe, welche die erste Verteidigungslinie überwinden oder sogar aus dem Innern des Netzwerks kommen, müssen zuverlässig erkannt und rasch unter Kontrolle gebracht werden, um die negativen Auswirkungen auf das übrige Netzwerk so gering wie möglich zu halten. Neben der erforderlichen Sicherheit muss das Netzwerk aber auch weiterhin die wichtigen Dienste bieten, die von den Benutzern erwartet werden. Eine solide Netzwerksicherheit in Verbindung mit einer guten Netzwerkfunktionalität ist möglich. Die SAFE-Architektur stellt kein revolutionär neues Konzept für das Netzwerkdesign dar, sondern ist als Vorlage für eine sichere Gestaltung bestimmt.

Die SAFE-Architektur für kleine bis mittelgroße Unternehmen und Remote-Netzwerke wurde ohne Fehlertoleranz gestaltet. Leser, die sich für die Gestaltung sicherer Netzwerke in einer fehlertoleranten Umgebung interessieren, werden auf das usprüngliche SAFE White Paper (im folgenden als ‚SAFE Enterprise' bezeichnet) verwiesen.

Im Netzwerkdesign stellt sich immer wieder die Frage, ob besser integrierte Funktionalität in einem Netzwerkgerät oder ein Dienstgerät mit einer speziellen Funktion eingesetzt werden soll. In vielen Fällen scheint die integrierte Funktionalität wohl die bessere Wahl zu sein, da sie in vorhandenen Geräten implementiert werden kann oder die Funktionen mit dem übrigen Gerät zusammenwirken können. Dienstgeräte dagegen werden häufig verwendet, wenn sehr weit reichende Funktionen erforderlich sind und/oder aufgrund der Leistungsanforderungen der Einsatz spezieller Hardware unumgänglich ist. So müssen Entscheidungen von Fall zu Fall unter Berücksichtigung der Kapazität und Funktionalität des Dienstgerätes gegenüber dem Integrationsvorteil des Netzwerkgerätes getroffen werden. So kann beispielsweise

anstelle eines kleineren IOS-Routers mit separater Firewall ein integrierter IOS-Router mit höherer Kapazität und IOS-Firewall-Software gewählt werden. Innerhalb der SAFE-Architektur kommen beide Lösungsansätze zur Anwendung. Wo die Gestaltungsanforderungen nicht eine bestimmte Lösung vorschrieben, wurde eine integrierte Funktionalität gewählt, um die Gesamtkosten der Lösung niedrig zu halten.

Modulares Konzept

Obwohl die meisten Netzwerke mit den steigenden IT-Anforderungen von Unternehmen weiterentwickelt werden, beruht die SAFE-Architektur auf einem modularen, von Grund auf neuen Ansatz. Dieser hat zwei wichtige Vorteile: Zum einen berücksichtigt die Architektur die Sicherheitsbeziehungen zwischen den einzelnen Funktionsblöcken des Netzwerks. Zum anderen haben Designer die Möglichkeit, Sicherheitsmechanismen Modul für Modul zu bewerten und einzusetzen, ohne die Architektur in nur einem Schritt bewältigen zu müssen. Das Sicherheitsdesign für jedes Modul wird einzeln beschrieben. Dennoch werden die Module als Teil des Gesamtdesigns betrachtet.

Die meisten Netzwerke können nicht ohne weiteres in klar definierte Module aufgeteilt werden. Dennoch stellt dieser Ansatz eine Orientierungshilfe zur Verfügung, um verschiedene Sicherheitsfunktionen innerhalb des Netzwerks zu implementieren. Netzwerk-Ingenieure sind nicht verpflichtet, ihre Netzwerke exakt nach den Vorgaben der SAFE-Implementierung aufzubauen. Vielmehr sollte eine Kombination der beschriebenen Module in bestehende Netzwerke integriert werden.

SAFE Axiome

Router sind Angriffsziele

Router steuern den Zugang von einem Netzwerk auf ein anderes. Sie werben für Netzwerke und filtern zulässige Benutzer. Sie sind auch die besten Freunde der Hacker. Router stellen daher ein kritisches Element in jeder Sicherungsstrategie dar. Sie haben grundsätzlich die Aufgabe, Zugriffe zu ermöglichen. Deshalb müssen sie gegen direkte Kompromittierung gesichert werden. Zu diesem Sicherheitsaspekt wurden bereits mehrere Dokumente verfasst, die nähere Erläuterungen zu den folgenden Themen enthalten:

- Sperren des Telnet-Zugriffs auf einen Router
- Sperren des SNMP-Zugriffs (Simple Network Management Protocol) auf einen Router
- Steuern des Zugriffs auf einen Router unter Verwendung von TACACS+ (Terminal Access Controller Access Control System Plus)
- Deaktivieren nicht benötigter Dienste
- Protokollieren auf entsprechenden Ebenen
- Authentifizierung von Routing-Updates

Switches sind Angriffsziele

Ebenso wie Router sind auch Switches (sowohl Layer-2 als auch Layer-3) besonderen Sicherheitsrisiken ausgesetzt. In diesem Fall sind jedoch weniger Informationen zu Sicherheitsrisiken und möglichen Abwehrmaßnahmen öffentlich zugänglich als für Router. Die meisten im vorangegangenen Abschnitt über Router genannten Sicherheitstechniken sind auch auf Switches anwendbar. Zusätzlich sind folgende Maßnahmen zu empfehlen:

- Für Ports, für die keine Trunk-Funktionalität erforderlich ist, sollten alle Trunk-Einstellungen deaktiviert werden – also nicht auf Auto gesetzt sein. Dies verhindert, dass ein Host zu einem Trunk-Port wird und den gesamten Datenverkehr empfängt, der normalerweise zu einem Trunk-Port gelangt.
- Wenn Sie ältere Software-Versionen für Ihren Ethernet-Switch verwenden, sollten den Trunk-Ports innerhalb des Switches eindeutige VLAN-Nummern (Virtual Local Area Network) zugewiesen werden. So lässt sich vermeiden, dass Pakete, die mit demselben VLAN markiert sind wie der Trunk-Port, ein anderes VLAN erreichen, ohne ein Layer-3-Gerät passieren zu müssen.
- Alle ungenutzten Ports eines Switches sollten deaktiviert werden. Dies verhindert, dass sich Hacker an ungenutzte Ports anschließen und mit dem übrigen Netzwerk kommunizieren.
- Verlassen Sie sich zur Sicherung des Zugriffs zwischen zwei Subnetzen nicht auf VLANs. Angesichts der Tatsache, dass hier ein großes Fehlerpotenzial im Hinblick auf menschliches Versagen besteht und außerdem bei der Konzeption von VLANs und VLAN-Tagging-Protokollen Sicherheitsfragen nicht in Betracht gezogen wurden, ist die Verwendung von VLANs in sensiblen Umgebungen nicht zu empfehlen. Wenn VLANs als Sicherheitsmechanismen erforderlich sind, beachten Sie die oben genannten Konfigurationen und Richtlinien sehr genau.

Innerhalb eines bestehenden VLANs bieten private VLANs in bestimmten Maße zusätzliche Sicherheit für bestimmte Netzwerk-Applikationen. Ihre Funktionsweise besteht darin, dass sie nur eine Kommunikation zwischen bestimmten Ports innerhalb eines VLANs und anderen Ports innerhalb desselben VLANs zulassen. Isolierte Ports innerhalb eines VLANs können nur mit Ports im Promiscuous-Mode kommunizieren. Community-Ports können nur mit Mitgliedern derselben Community sowie mit Ports im Promiscuous-Mode kommunizieren. Ports im Promiscuous-Mode können mit jedem beliebigen Port kommunizieren. Auf diese Weise kann ein einzelner kompromittierter Host keinen großen Schaden anrichten. Stellen Sie sich ein Standardsegment für öffentliche Dienste mit einem Web-Server, FTP-Server (File Transfer Protocol) und einem DNS-Server (Domain Name System) vor. Wenn der DNS-Server kompromittiert wird, kann ein Hacker die beiden anderen Ports angreifen, ohne von einer Firewall aufgehalten zu werden. Mit dem Einsatz von privaten VLAN kann ein kompromittiertes System nicht mit den anderen Systemen kommunizieren. Den einzigen Angriffszielen, denen ein Hacker nachgehen kann, sind Hosts hinter der Firewall. Weil sie die Layer-2-Konnektivität einschränken, erschweren private VLAN die Fehlersuche bei Netzwerkproblemen. Vergessen Sie nicht, dass private VLAN nicht von allen auf den Markt erhältlichen Switches unterstützt werden. Speziell Low-End-Switches unterstützen diese Funktion bislang nicht.

Hosts sind Angriffsziele

Hosts stellen das beliebteste Angriffsziel dar und sind gleichzeitig am schwierigsten zu schützen. Es gibt zahlreiche Hardwareplattformen, Betriebssysteme und Anwendungen, für die jeweils zu unterschiedlichen Zeiten Updates, Patches und Fehlerkorrekturen erhältlich sind. Da Hosts anderen Hosts die von diesen angeforderte Applikationsdienste zur Verfügung stellen, sind sie innerhalb des Netzwerks sehr exponiert. Viele Menschen haben beispielsweise **www.whitehouse.gov** besucht, einen Host. Nur wenige haben hingegen versucht, auf s2-0.whitehouseisp.net zuzugreifen – einen Router. Aufgrund dieser Sichtbarkeit werden Hosts bei unbefugten Zugriffsversuchen weitaus häufiger angegriffen als andere Netzwerkgeräte. Angriffe verlaufen hier zusätzlich am erfolgreichsten, teilweise aufgrund der oben genannten Probleme. Es kann zum Beispiel vorkommen, dass auf einem bestimmten Webserver im Internet eine Hardwareplattform eines Herstellers, ein Netzwerkadapter eines anderen Herstellers, ein Betriebssystem wieder eines anderen Herstellers und eine Webserver-Software, die entweder ein Open-Source-Produkt oder das Produkt wieder eines anderen Herstellers ist, verwendet wird. Zusätzlich könnten auf demselben Webserver Applikationen ausgeführt werden, die frei über das Internet verteilt werden. Der Webserver könnte dann mit einem Datenbankserver kommunizieren, der aus ebenso unterschiedlichen Komponenten zusammengesetzt ist. Damit soll nicht behauptet werden, dass Schwachpunkte in Fragen der Sicherheit in besonderem Maße von der Verwendung von Produkten verschiedener Hersteller herrühren. Mit zunehmender Komplexität eines Systems nimmt aber auch die Wahrscheinlichkeit eines Ausfalls oder Fehlers zu.

Zur Sicherung von Hosts müssen alle Systemkomponenten mit besonderer Sorgfalt ausgewählt werden. Installieren Sie für alle Systeme die neuesten Patches, Fehlerkorrekturen und so weiter. Beachten Sie besonders, wie diese Patches den Betrieb der anderen Systemkomponenten beeinflussen. Prüfen Sie alle Updates vor der Implementierung in einer Produktionsumgebung auf Testsystemen. Wenn Sie dies nicht tun, könnte der Patch selbst einen DoS-Angriff (Denial of Service) verursachen.

Netzwerke sind Angriffsziele

Angriffe auf ein Netzwerk sind sehr schwierig abzuwehren, weil sie die spezifischen Eigenarten von Netzwerken ausnutzen. Zu diesen Angriffen gehören ARP- und MAC-basierte Angriffe (Address Resolution Protocol und Media Access Control) in Layer-2-, Sniffer- und DDos-Attacken. Einige der ARP- und MAC-basierten Layer-2-Angriffe können durch optimale Einstellungen der Router und Switches abgewehrt werden. DDoS-Angriffe sind jedoch einzigartig und bedürfen besonderer Beachtung.

Die schlimmsten Angriffe sind die, die unaufhaltsam ihren Lauf nehmen. Ein richtig ausgeführter DDoS ist so ein Angriff. Hierbei werden Dutzende oder sogar Hunderte von Computern veranlasst, gleichzeitig falsche Daten an eine IP-Adresse zu senden. In der Regel zielen die Urheber eines solchen Angriffs nicht darauf ab, einen bestimmten Host zum Absturz zu bringen, sondern das gesamte Netzwerk lahm zu legen. Denken Sie zum Beispiel an ein Unternehmen, das über eine DS1-Verbindung mit 1.5 Mbit/s zum Internet verfügt und Benutzern auf seiner Webseite E-Commerce-Dienste anbietet. Eine solche Seite ist sehr sicherheitsbewusst angelegt und mit Angriffserkennung, Firewalls, Protokollierfunktionen und aktivem Monitoring ausgestattet. Leider greifen diese Sicherheitsvorkehrungen nicht, wenn ein Hacker einen erfolgreichen DDoS-Angriff durchführt.

Wenn 100 Geräte in aller Welt mit einer DSL-Verbindung mit 500 Kbit/s zum Internet von einem entfernten Standort die Anweisung erhalten, die serielle Schnittstelle des Internet-Routers des Unternehmens mit Daten zu überschütten, kann dabei problemlos die DS1-Verbindung mit falschen Daten überflutet werden. Selbst wenn jeder Host nur Datenverkehr mit 100 Kbit/s (Labortests deuten darauf hin, dass ein handelsüblicher PC ohne weiteres 50 Mbit/s mit einem beliebten DDoS-Tool erzielen kann) erzeugt, ist die Datenmenge immer noch doppelt so groß wie die, die die E-Commerce-Seite verarbeiten könnte. Das führt dazu, dass legitime Web-Anforderungen verloren gehen und die Seite für die meisten Benutzer ausgefallen zu sein scheint. Die lokale Firewall weist theoretisch alle falschen Daten zurück, aber zu diesem Zeitpunkt ist der Schaden schon eingetreten. Die Daten haben die WAN-Verbindung bereits passiert und die Verbindung blockiert.

Das fiktive E-Commerce-Unternehmen hat nur in Zusammenarbeit mit seinem ISP (Internet Service Provider) die Möglichkeit, Angriffe zu vereiteln. Der ISP kann für die Ausgangsschnittstelle der Unternehmensseite eine Ratenbegrenzung konfigurieren. Mit dieser Begrenzung kann der größte Teil des unerwünschten Datenverkehrs zurückgewiesen werden, sobald dieser mehr als einen festgelegten Teil der verfügbaren Bandbreite einnimmt. Das Wichtigste ist, Daten eindeutig als unerwünscht zu kennzeichnen.

Häufig verwendete Formen von DDoS-Tools arbeiten mit ICMP- (Internet Control Message Protocol), TCP SYN- oder UDP-Flooding (User Datagram Protocol). In einer E-Commerce-Umgebung ist diese Art von Datenverkehr einfach zu kategorisieren. Die einzige Gefahr besteht darin, dass der Administrator durch die Begrenzung von TCP SYN-Angriffen auf Port 80 (HTTP, Hyper Text Transfer Protocol) während eines Angriffs Zugriffe durch legitime Benutzer unterdrückt. Selbst dann ist es besser, neue legitime Benutzer vorübergehend zu sperren und dafür Routing- und Managementverbindungen zu erhalten, als einen Angriff auf den Router zuzulassen und dadurch jegliche Anbindung einzubüßen.

Bei ausgeklügelteren Angriffen wird Datenverkehr an Port 80 mit gesetztem ACK-Bit verwendet, sodass dieser wie legitimer Webverkehr aussieht. Dass ein Administrator einen solchen Angriff richtig kategorisieren kann, ist sehr unwahrscheinlich. TCP-Kommunikationen mit Bestätigungen lässt schließlich jeder gerne in sein Netzwerk.

Eine Möglichkeit, solche Angriffe abzuwehren, ist die Befolgung von Filterrichtlinien für Netzwerke, die in RFC 1918 und RFC 2827 niedergelegt sind. Dabei werden in RFC 1918 die Netzwerke benannt, die der privaten Verwendung vorbehalten sind und im öffentlichen Internet niemals sichtbar sein sollten. Die Filterung nach RFC 1918 und 2827 sollte beispielsweise in Form von Eingangsfiltern an mit dem Internet verbundenen Routern eingesetzt werden, um zu verhindern, dass unerlaubter Datenverkehr das Unternehmensnetzwerk erreicht. Bei Implementierung auf Seiten des ISP lässt sich mit Hilfe der Filterung verhindern, dass DDoS-Angriffspakete, die diese Adressen als Absender verwenden, die WAN-Verbindung passieren. Dadurch kann während des Angriffs gegebenenfalls Bandbreite gespart werden. Würden alle ISPs auf der Welt die in RFC 2827 dargelegten Richtlinien umsetzen, ließe sich das Spoofing von Herkunftsadressen erheblich reduzieren. Damit wäre es zwar immer noch nicht möglich, DDoS-Attacken von vornherein zu unterbinden, jedoch könnte die Absenderadresse eines solchen Angriffs nicht mehr getarnt werden und eine Rückverfolgung zu den angreifenden Netzen würde erheblich einfacher. Fragen Sie Ihren ISP, welche Abwehrmöglichkeiten er zur Verfügung stellt.

Applikationen sind Angriffsziele

Applikationen werden größtenteils von Menschen codiert und sind von Natur aus ziemlich fehleranfällig. Solche Fehler können gutartig sein, wenn beispielsweise ein Dokument ungenau ausgedruckt wird. Schwerwiegend sind sie, wenn Kreditkartennummern auf dem Datenbankserver per Anonymous FTP abgerufen werden können. Diese Probleme sowie eine Reihe anderer, allgemeiner Sicherheitsprobleme müssen sehr genau beobachtet werden. Um sicherzustellen, dass kommerzielle und frei zugängliche Anwendungen mit den allerneusten Fehlerkorrekturen ausgestattet sind, ist große Sorgfalt erforderlich. Frei zugängliche Anwendungen sowie individuell entwickelte Applikationen müssen auf ihren Code hin überprüft werden. So wird sichergestellt, dass Anwendungen keine Sicherheitsrisiken darstellen, weil sie schlecht programmiert wurden. Zum Beispiel kann eine Anwendung so programmiert werden, dass sie mit anderen Anwendungen oder dem Betriebssystem kommuniziert. Dazu gehört auch das Ausmaß der Privilegien, das Vertrauen in die umgebenden Systeme sowie die Methode des Datentransports. Der folgende Abschnitt dreht sich um IDS (Intrusion Detection Systeme) und wie sie Angriffe gegen Anwendungen und andere Funktionen innerhalb des Netzwerks abwehren können.

Intrusion Detection Systeme

Intrusion Detection Systeme funktionieren wie eine Alarmanlage in der realen Welt. Sobald das IDS etwas erkennt, das es als Angriff wertet, kann es entweder selbständig entsprechende Maßnahmen ergreifen oder eine Mitteilung an ein Managementsystem senden, damit der Administrator entsprechende Schritte einleiten kann. Manche Systeme sind mehr oder weniger in der Lage, auf solche Angriffe zu reagieren und diese zu vereiteln. Die host-basierte Angriffserkennung kann Betriebssystem- und Applikationsaufrufe auf einzelnen Hosts abfangen. Alternativ kann ein solches IDS auch nachträglich lokale Protokolldateien analysieren. Im ersten Fall können Angriffe besser vereitelt werden, während im zweiten Fall die Reaktion auf einen Angriff eher passiv ausfällt. Aufgrund ihrer besonderen Rolle sind host-basierte IDS (HIDS) im Vergleich zu Netzwerk-IDS (NIDS) oft besser geeignet, bestimmte Angriffe zu vereiteln, als einfach nur eine Warnung bei Erkennen eines Angriffs auszugeben. Durch diese Eigenheit geht jedoch die Perspektive für das Netz als Ganzes verloren. In diesem Bereich glänzen NIDS. Cisco empfiehlt daher als umfassendes Angriffserkennungssystem eine Kombination der beiden Systeme: HIDS auf kritischen Hosts und NIDS für das gesamte Netzwerk. Leider geben IT-Etats oft vor, dass entweder die eine oder die andere Lösung angeschafft wird. In diesem Fall sollten die Gesamtkosten jeder Technologie, die Anzahl der Geräte, die überwacht werden müssen und das Personal, das erforderlich ist, um bei einem Angriff zu reagieren, genau kalkuliert werden.

Nach der anfänglichen Einrichtung muss jede IDS-Implementierung fein abgestimmt werden, um ihre Effektivität zu steigern und Fehlalarme zu vermeiden. Bei Fehlalarmen handelt es sich um Alarme, die fälschlicherweise durch legitimen Datenverkehr beziehungsweise legitime Aktivitäten ausgelöst wurden. Als Fehlzulassung hingegen werden Angriffe bezeichnet, die das IDS nicht erkennt. Nach einer Feinabstimmung des IDS kann dieses gezielter für seine Aufgabe zur Gefahrenabwehr konfiguriert werden. Wie bereits erwähnt, sollte das HIDS so konfiguriert werden, dass die meisten realen Bedrohungen auf Hostebene abgefangen werden können. Dieses System bietet die beste Voraussetzung, um eine bestimmte Aktivität als tatsächliche Bedrohung zu erkennen.

Bei jeder Entscheidung in Bezug auf die Aufgaben von NIDS in der Sicherheit gibt es im Wesentlichen zwei Möglichkeiten. Erinnern Sie sich, dass der allererste Schritt vor der Implementierung einer Abwehrfunktion die genaue Feinabstimmung des NIDS ist, um sicherzustellen, dass jede erkannte Gefahr legitim ist.

Die erste Möglichkeit, die bei falscher Verwendung potenziell den größten Schaden anrichten kann, besteht darin, Datenverkehr „auszugrenzen“, indem Router und Firewalls zusätzlich mit Zugangskontrollfiltern ausgestattet werden. Wenn ein NIDS einen Angriff von einem bestimmten Host über ein bestimmtes Protokoll erkennt, kann es den betreffenden Host für einen zuvor festgelegten Zeitraum daran hindern, auf das Netzwerk zuzugreifen. Auf den ersten Blick erscheint diese Methode als wertvolles Instrument für den Systemadministrator. Er muss jedoch bei der Implementierung größte Vorsicht walten lassen, wenn er nicht sogar ganz auf die Implementierung verzichtet. Das erste Problem ist das Verschleiern von Adressen. Erkennt das NIDS Daten, die es als Angriff wertet, sodass durch den entsprechenden Alarm eine Ausgrenzungssituation ausgelöst wird, kommt die Zugangsliste für das Gerät zum Einsatz. Wenn nun aber bei dem Angriff, der den Alarm ausgelöst hat, eine verschleierte Adresse verwendet wurde, hat das NIDS eine Adresse gesperrt, von der niemals ein Angriff ausgegangen ist. Handelt es sich bei der von dem Hacker verwendeten IP-Adresse um die IP-Adresse des für den abgehenden Datenverkehr zuständigen HTTP-Proxyservers eines großen ISP, kann es sogar passieren, dass unzählige Benutzer gesperrt werden. Das allein könnte für kreative Hacker schon als Anreiz für einen DoS-Angriff ausreichen.

Um die Risiken des Ausgrenzungsverfahrens möglichst gering zu halten, sollte diese Methode grundsätzlich nur bei TCP-Datenverkehr angewendet werden. Hier ist erfolgreiches Spoofing sehr viel schwieriger als bei UDP. Setzen Sie sie nur in Fällen einer realen Bedrohung ein, wenn also die Gefahr, dass es sich bei einem erkannten Angriff eigentlich um einen Fehlalarm handelt, sehr gering ist. Das Ausgrenzungsverfahren sollte möglichst kurz gehalten werden. Der Benutzer wird so lange ausgegrenzt, bis der Administrator entschieden hat, welche dauerhaften Maßnahmen – wenn überhaupt – gegen diese IP-Adresse ergriffen werden. Innerhalb eines Netzwerks gibt es jedoch noch zahlreiche weitere Möglichkeiten. Mit dem effektiven Einsatz der Filterung nach RFC 2827 lässt sich Spoofing weitgehend unterbinden. Zudem können auch Angriffe aus dem internen Netzwerk strenger unterbunden werden, da sich Kunden in der Regel nicht im internen Netzwerk befinden. Dabei fällt auch ins Gewicht, dass interne Netzwerke häufig nicht über so statusbetonte Filtermechanismen verfügen wie Edge-Verbindungen. Aus diesem Grund kommt hier dem IDS eine wesentlich wichtigere Rolle zu als in der externen Umgebung.

Die zweite Möglichkeit zur Abwehr von Bedrohungen mittels NIDS ist die Verwendung von TCP-Resets. Wie der Name schon sagt, funktionieren TCP-Resets nur bei TCP-Datenverkehr. Dabei werden aktive Angriffe beendet, indem TCP-Resetmeldungen sowohl an den angreifenden als auch an den angegriffenen Host gesendet werden. Da sich das Spoofing von TCP-Datenverkehr als schwieriger gestaltet, ist die Verwendung von TCP-Resets in vielen Fällen eher zu empfehlen als das Ausgrenzungsverfahren. Berücksichtigen Sie, dass TCP-Resets im Vergleich zu Standard-Hubs aufwändiger sind, wenn sie in einer geswitchten Umgebung durchgeführt werden. Ohne SPAN (Switched Port Analyser) oder gespiegelte Ports erkennen Ports nicht den gesamten Datenverkehr. Stellen Sie sicher, dass der gespiegelte Port den bidirektionalen Datenverkehr unterstützt und dass bei ihm das Erkennen der MAC-Adresse auf dem SPAN-Port deaktiviert werden kann.

Die IDS-Konsolen müssen bei beiden Abwehrmöglichkeiten rund um die Uhr vom Personal überwacht werden. Weil die IT-Mitarbeiter, vor allem in kleineren Unternehmen, oft überarbeitet sind, ist es sinnvoll, Ihr IDS-Management auf einen externen Anbieter auszulagern.

Unter dem Aspekt der Leistung muss berücksichtigt werden, dass ein NIDS Pakete bei der Übertragung überwacht. Werden die Pakete schneller gesendet, als sie das NIDS verarbeiten kann, hat das keinen negativen Einfluss auf die Netzwerkleistung, denn das NIDS befindet sich nicht unmittelbar im Datenfluss. Allerdings kann das NIDS dann nicht mehr so effektiv arbeiten und Pakete können übersehen werden. Dadurch kann es sowohl zu Fehlalarmen als auch zu nicht erkannten Angriffen kommen. Achten Sie darauf, dass die Kapazität eines IDS ausreichend hoch ist, damit alle Vorteile voll ausgenutzt werden können. Unter dem Aspekt des Routing ist zu beachten, dass IDS ebenso wie viele statusorientierte Engines in Umgebungen mit asymmetrischem Routing nicht einwandfrei arbeiten. Wenn Pakete über eine Gruppe von Routern und Switches nach außen gesendet werden, jedoch über eine andere Gruppe von Routern und Switches zurück kommen, hat dies zur Folge, dass die IDS nur die Hälfte des Datenverkehrs sehen und daher Fehlalarme ausgeben oder echte Angriffe nicht erkennen.

Management und Reporting von Sicherheit

„Wenn du etwas protokollierst, lies es auch.“ Diese Aussage ist so einfach, dass sie fast alle, die sich mit Netzwerksicherheit auskennen, schon einmal getroffen haben. Das Protokollieren und Auswerten von Informationen aus vielen Geräten kann jedoch eine große Herausforderung darstellen. Welche Aufzeichnungen sind wichtig? Wie kann ich wichtige Nachrichten von unwichtigen Benachrichtigungen unterscheiden? Wie kann ich sicherstellen, dass sich niemand an den Daten zu schaffen macht, wenn sie unterwegs sind? Wie kann ich sicherstellen, dass meine Zeitstempel übereinstimmen, wenn mehrere Geräte den gleichen Alarm anzeigen? Welche Informationen werden benötigt, wenn Protokolldaten kriminalpolizeilich angefordert werden? Wie kann ich die Masse an Nachrichten bewältigen, die entsteht, wenn ein System angegriffen wird? Diese Fragen müssen berücksichtigt werden, wenn Log-Files effektiv verwaltet werden sollen. Unter dem Management-Aspekt müssen andere Fragen gestellt werden: Wie verwalte ich ein Gerät sicher? Wie kann ich Inhalte an öffentliche Server übertragen und sicherstellen, dass sie bei der Übertragung nicht verändert werden? Wie kann ich Änderungen an den Geräten verfolgen, um nachzuvollziehen, wenn Angriffe oder Fehler im Netzwerk auftreten?

Die Architektur für das „Out-of-Band“-Management (OOB), die in SAFE Enterprise beschrieben wird, liefert ein sehr hohes Maß an Sicherheit. Dennoch wird es hier nicht empfohlen, weil der kostengünstige Einsatz von Sicherheitskomponenten Priorität hat. In der OOB-Umgebung hat jedes Netzwerkgerät und jeder Host seine eigene dezidierte Management-Schnittstelle, über die sie mit dem privaten Netzwerk verbunden sind. Dieser Aufbau senkt das Risiko, dass unsichere Management-Protokolle wie Telnet, TFTP (Trivial File Transfer Protocol), SNMP und syslog in das Produktionsnetzwerk gelangen können, wo es unterbrochen oder abgeändert werden könnte. Der Management-Datenverkehr fließt in der hier beschriebenen Architektur in jedem Fall „in-Band“. Mit Tunnelling-Protokollen und sicheren Varianten unsicherer Management-Protokolle wird bestmöglich geschützt. So wird zum Beispiel – wenn möglich – SSH (Secure Shell Protocol) statt Telnet eingesetzt. Wenn der Management-Datenverkehr „in-Band“ durch das Produktionsnetzwerk fließt, wird es zunehmend wichtig, die Axiome noch genauer zu verfolgen, die weiter vorne angesprochen wurden.

Wenn ein Gerät, das sich außerhalb einer Firewall befindet, verwaltet werden muss, sollten Sie mehrere Aspekte berücksichtigen. Zunächst: welche Management-Protokolle unterstützt das Gerät?

Für Geräte, die IPSec (IP Security) unterstützen, sollten die Geräte verwaltet werden, indem einfach ein Tunnel vom Management-Netzwerk zum Gerät aufgebaut wird. Damit können viele unsichere Management-Protokolle über einen einzigen verschlüsselten Tunnel übertragen werden. Ist IPSec nicht möglich, da es vom Gerät nicht unterstützt wird, müssen andere, weniger sichere Alternativen gefunden werden. SSH oder SSL (Secure Sockets Layer) können anstelle von Telnet häufig zur Konfiguration des Geräts verwendet werden. Damit können alle Änderungen in der Konfiguration des Geräts verschlüsselt werden. Die gleichen Protokolle können anstelle von unsicheren Protokollen wie TFTP und FTP zum Teil verwendet werden, um Daten zu einem Gerät zu senden und von dort zu übertragen. TFTP wird dennoch für Cisco-Produkte zur Konfigurierung oder Aktualisierung von Software-Versionen benötigt.

Dies führt zur zweiten Frage: Muss der Management-Kanal zu jeder Zeit aktiv sein? Wenn nicht, können temporäre Löcher in die Firewall gesetzt werden, während die Management-Funktionen ausgeführt werden. Die Löcher werden später wieder entfernt. Dieser Vorgang ist allerdings nicht auf eine große Zahl an Geräten skalierbar. Wenn der Kanal wie beispielsweise für SNMP ständig aktiv sein muss, sollten Sie sich die dritte Frage stellen: Brauchen Sie dieses Management-Tool wirklich? SNMP-Manager werden oft innerhalb eines Netzwerks benötigt, um Fehlersuche und Konfiguration zu erleichtern. Ist das für einen DMZ-Switch, der Layer-2-Dienste für zwei oder drei Server liefert, wirklich erforderlich? Wenn nicht, deaktivieren Sie ihn. Wenn Sie entscheiden, dass er wichtig ist, denken Sie daran, dass Sie eine potenzielle Schwachstelle in Ihre Umgebung integrieren. Die nächsten Abschnitte erläutern die spezifischen Management-Arten im Detail.

Unter dem Aspekt des Reporting können die meisten Netzwerkgeräte syslog-Daten versenden, die unbezahlbar sind, wenn es um die Fehlersuche in Netzwerken oder das Erkennen von Sicherheitsgefahren geht. Senden Sie diese Daten von jedem Gerät, dessen Protokolle Sie einsehen möchten, an den Host, der Ihre Protokolldaten auswertet. Diese Daten können zeitgleich oder über angeforderte und zusammengestellte Berichte eingesehen werden. Je nach Gerät können Sie aus mehreren Protokollebenen auswählen, damit die richtige Anzahl an Daten zu Ihrem Protokolliergerät gesendet wird. Zum exakten Betrachten und für das Reporting müssen die Logdaten des Geräts innerhalb der Auswertungs-Software gekennzeichnet werden. Während eines Angriffs können beispielsweise die Daten, die das IDS bereitstellt, mehr Aufschluss geben als die Log-Dateien der Layer-2-Switches. Um sicherzustellen, dass die Nachrichten aus den Protokoll-Dateien untereinander zeitgleich sind, müssen die Uhren auf Hosts und Netzwerkgeräten übereinstimmen. Mit dem NTP (Network Time Protocol) ist die Uhrzeit auf allen Geräten, die das Protokoll unterstützen, gleich. Bei der Analyse von Angriffen geht es um Sekunden, da es wichtig ist, den zeitlichen Ablauf eines Angriffs zu erkennen.

Das Management der Konfigurationsänderungen ist ein anderes Thema, das mit sicherem Management verwandt ist. Wird ein Netzwerk angegriffen, ist es wichtig zu wissen, wie der Zustand der kritischen Netzwerkgeräte ist und wann die letzten bekannten Änderungen vorgenommen wurden. Ein Plan zum Change Management sollte Teil Ihrer Sicherheitspolicy sein. Sie sollten zumindest Änderungen mit Authentifizierungs-Systemen auf den Geräten aufzeichnen und Konfigurationen mittels FTP oder TFTP archivieren.

Head-End- oder Zweigstellen-Design?

Die nachfolgend dargestellten kleinen und mittelgroßen Netzwerkdesigns sind in zwei Konfigurationen denkbar. In der ersten Konfiguration ist das Design die ‚Kopfstation' (Head-End) des Unternehmensnetzwerkes. Dieses Head-End kann VPN-Verbindungen zu anderen Niederlassungen desselben Unternehmens haben. So kann beispielsweise eine große Anwaltskanzlei das mittelgroße Netzwerkdesign als Head-End und mehrere kleine Netzwerkdesigns für ihre anderen Büros verwenden. Vollzeit-Heimarbeiter können über einige der im Zusammenhang mit dem Remote-Netzwerkdesign beschriebenen Anbindungen an das Head-End angeschlossen werden. In der zweiten Konfiguration dient das Design als Zweigstelle einer größeren Organisation, die gemäß der Beschreibung im ‚SAFE Enterprise'-Dokument konfiguriert ist.

Als ein weiteres Beispiel wäre ein großes Automobilwerk vorstellbar, welches das SAFE Enterprise-Design für seine Zentrale und die verschiedenen, im vorliegenden Dokument beschriebenen Designs für seine Zweigstellen und Heimarbeiter verwendet. Änderungen des konkreten Designs können von Fall zu Fall erforderlich sein und werden in dem entsprechenden Kontext beschrieben.

Erwartete Sicherheitsrisiken

Aus der Perspektive des Sicherheitsrisikos verhält sich ein kleines oder mittelgroßes Netzwerk wie die meisten anderen Netzwerke mit Anbindung an das Internet –– einige interne Benutzer benötigen den Zugang nach draußen, und einige externe Benutzer benötigen den Zugang nach drinnen. Mehrere gebräuchliche Risiken können eine erste Kompromittierung verursachen, nach der ein Hacker durch sekundäre Angriffe weiter in das Netzwerk vordringen kann.

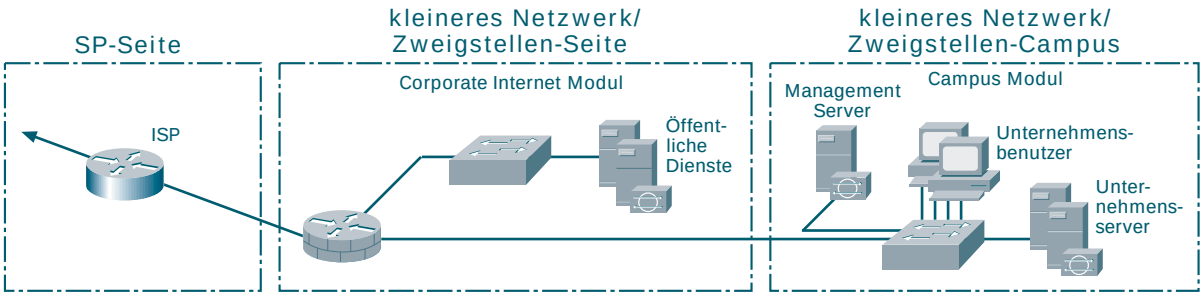
Zunächst ist eine Bedrohung durch interne Benutzer denkbar. Obwohl die Statistiken über den konkreten Prozentsatz stark auseinander gehen, gilt es als erwiesen, dass die meisten Attacken aus dem internen Netzwerk kommen. Verärgerte Mitarbeiter, Spione im Unternehmen, Besucher und ohne böse Absicht im Netz herumstöbernde Mitarbeiter sind potenzielle Quellen solcher Angriffe. Bei der Gestaltung der Sicherheit muss eine mögliche Bedrohung von innen in Betracht gezogen werden.

Zweitens kann eine Bedrohung für die öffentlich zugänglichen Hosts mit Anbindung an das Internet auftreten. Diese Systeme werden wahrscheinlich unter Ausnutzung von Sicherheitslücken im Application Layer und mit DoS-Attacken angegriffen.

Struktur eines kleineren Netzwerks

Das kleinere Netzwerkdesign besteht aus zwei Modulen: dem Corporate Internet Modul und dem Campus Modul. Das Corporate Internet Modul stellt die Anbindung an das Internet her und terminiert den Datenverkehr über VPN und öffentlich verfügbare Netzwerkdienste wie DNS, HTTP, FTP und SMTP. Das Campus Modul stellt Layer-2-Switching-Funktionen zur Verfügung und bindet alle Benutzer sowie die Management- und Intranet-Server an. Die Beschreibung zu diesem Design basiert größtenteils auf einem kleinen Netzwerk, das als Head-End für ein Unternehmen eingesetzt wird. Wird es in Zweigstellen eingesetzt, wird auf die speziellen Änderungen eingegangen.

Abbildung 1: Detaillierte Ansicht eines kleineren Netzwerks.



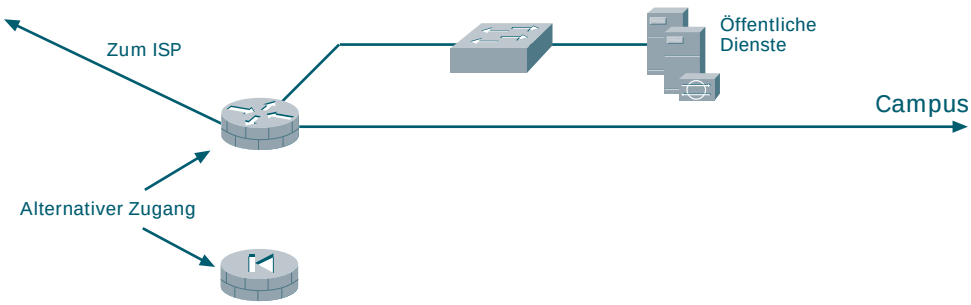
Corporate Internet Modul

Das Corporate Internet Modul stellt den internen Benutzern den Zugang zu Internet-Diensten zur Verfügung und ermöglicht den Internet-Benutzern Zugriff auf Informationen auf öffentlichen Servern. Außenstellen und Telearbeiter haben hier Zugang über VPN. Dieses Modul ist nicht dafür geeignet, E-Commerce-Anwendungen bereitzustellen. Im Abschnitt „E-Commerce-Modul“ in SAFE Enterprise erhalten Sie dazu mehr Informationen.

Hauptgeräte

- **SMTP Server**: Fungiert als Relais zwischen dem Internet und den Mailservern im Intranet.
- **DNS Server**: Dient als zuverlässiger externer DNS Server für das Unternehmen; leitet interne Anfragen an das Internet weiter.
- **FTP/HTTP Server**: Stellt öffentlich zugängliche Informationen über das Unternehmen zur Verfügung.
- **Firewall oder Firewall Router:** Schützt die Ressourcen und bietet Stateful-Filtering des Datenverkehrs sowie VPN-Terminierung auf Netzwerkebene für Außenstellen und mobile Benutzer.
- **Layer-2-Switch (mit Unterstützung von privaten VLAN):** Stellt sicher, dass die Daten aus den kritischen Systemen immer über die IOS Firewall laufen.

Abbildung 2: Detaillierte Ansicht des Corporate Internet Moduls für kleinere Netzwerke.

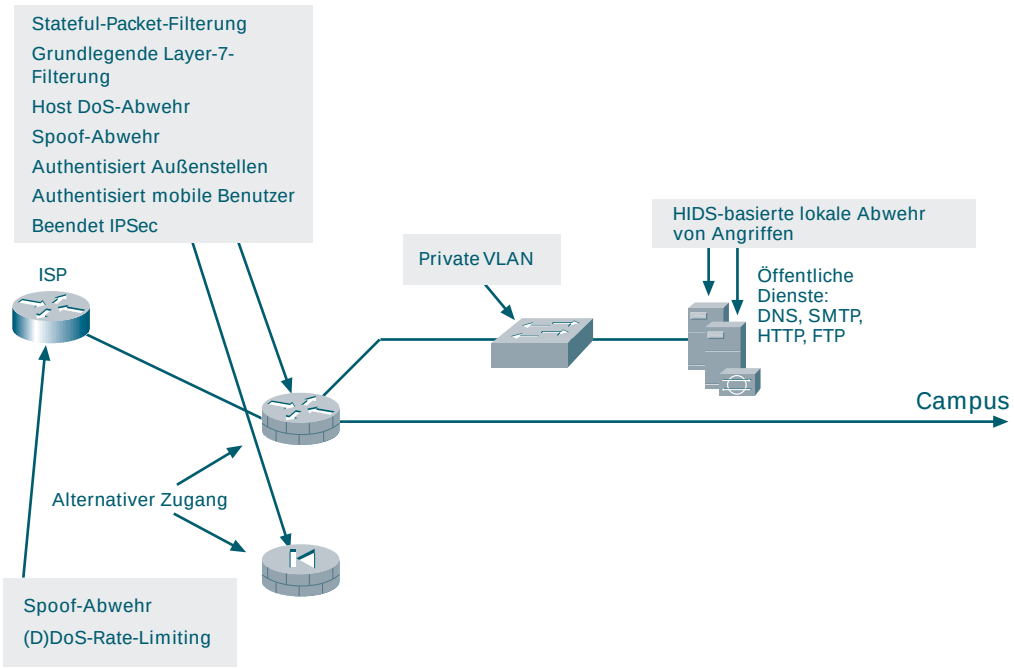


Folgende Angriffe werden abgewehrt:

An den öffentlich verfügbaren Server sind die meisten Angriffe zu erwarten. Sie sind folgenden Risiken ausgesetzt:

- **Unerlaubter Zugang:** Wird durch Filterung an der Firewall verhindert.
- **Angriffe in der Anwendungsschicht:** Werden mit HIDS auf den öffentlichen Servern abgewehrt.
- **Angriffe durch Viren und trojanische Pferde:** Werden durch Virenscanner auf Hostebene vermieden.
- **Passwort-Angriffe:** Verfügbare Dienste für Brute-Force-Angriffe sind eingeschränkt; Betriebssystem und Intrusion Detection System können die Gefahr erkennen.
- **DoS-Attacken:** Angriffsmöglichkeiten werden durch garantierte Zugangsdaten (CAR) auf der ISP-Seite und TCP-Setup-Kontrollen an der Firewall beschränkt.
- **IP-Spoofing:** Wird durch Filterung nach RFC 2827 und 1928 auf der ISP-Seite und auf der lokalen Firewall verhindert.
- **Packet Sniffer:** Gefahr wird durch geswitchte Infrastruktur und HIDS eingeschränkt.
- **Network Reconnaissance:** HIDS erkennt das Ausspionieren; Protokolle werden gefiltert, um die Effektivität zu reduzieren.
- **Trust Exploitation:** Wird durch restriktive Trust-Modelle sowie den Einsatz privater VLAN minimiert.
- **Umleitung von Ports:** Wird durch strenges Filtern und den Einsatz von HIDS verhindert.

Abbildung 3: Angriffsabwehr im Corporate Internet Modul in kleineren Netzwerken.



Gestaltungsrichtlinien

Dieses Modul ist das ultimative sicherheitsbewusste Netzwerkdesign in seiner kompaktesten Form: Alle erforderlichen Sicherheits- und VPN-Dienste sind in einem einzigen Gerät zusammengefasst. Für die Implementierung dieser Funktionalität bieten sich zwei grundlegende Alternativen an. Die erste besteht darin, einen Router mit Firewall und VPN-Funktionalität zu verwenden. Dies bietet die höchste Flexibilität für das kleine Netzwerk, da der Router alle weiterführenden Dienste (QoS, Routing, Multi-Protokoll-Support, usw.), die in den heutigen Netzwerken gefordert werden, unterstützt. Alternativ kann anstelle des Routers eine dedizierte Firewall eingesetzt werden. Aus dieser Anordnung ergeben sich einige Einschränkungen für den Einsatz. Zunächst einmal sind Firewalls üblicherweise nur für Ethernet ausgelegt, was eine Umsetzung des entsprechenden WAN-Protokolls erforderlich macht.

In den heutigen Netzwerkumgebungen werden die meisten Kabelmodems und DSL (Digital Subscriber Line) Router/Modems vom Service Provider gestellt und ermöglichen den Anschluss an die Firewall über Ethernet. Wenn am Gerät eine WAN-Anbindung erforderlich ist (z. B. bei einer DS1-Leitung eines TK-Anbieters), muss ein Router verwendet werden. Die Verwendung einer dedizierten Firewall bietet den Vorteil einer einfacheren Konfiguration der Sicherheitsdienste, und eine dedizierte Firewall bietet mehr Leistung bei den eigentlichen Firewall-Funktionen. Unabhängig davon, welches Gerät verwendet wird, erfolgt eine Stateful-Überprüfung des Datenverkehrs in alle Richtungen, damit nur zulässiger Datenverkehr über die Firewall übertragen wird. Bevor der Verkehr die Firewall erreicht, wird beim ISP im Idealfall bereits eine Sicherheitsfilterung vorgenommen. Man muss sich hierbei den Grundsatz vergegenwärtigen, dass Router naturgemäß den Datenverkehr zulassen, während Firewalls diesen standardmäßig blockieren sollen.

Ausgehend vom kundenseitigen Router beim ISP erfolgt am ISP-Ausgang eine Begrenzung der Übertragungsrate für unerwünschten Datenverkehr, der bestimmte Schwellenwerte überschreitet und wehrt damit DDoS-Angriffe ab. Ebenfalls am Ausgang des ISP-Routers wehrt eine RFC 1918- und RFC 2827-Filterung das Quelladressen-Spoofing in lokalen Netzwerken und privaten Adressbereichen ab.

Am Eingang der Firewall dient die RFC 1918- und RFC 2827-Filterung zunächst zur Verifizierung der ISP-Filterung. Wegen des enormen Sicherheitsrisikos durch fragmentierte Pakete wird die Firewall zusätzlich so konfiguriert, dass sie die meisten fragmentierten Pakete unterdrückt, die für die Standard-Übertragungsarten im Internet nicht typisch sind. Verluste von legalen Datenübertragungen durch diese Filterung werden angesichts des Risikos, das durch Zulassen dieses Datenverkehrs entstehen würde, als akzeptabel angesehen. Der von außen kommende und für die Firewall selbst bestimmte Verkehr wird auf IPSec-Verkehr und alle für das Routing erforderlichen Protokolle beschränkt.

Die Firewall bietet Connection-State-Enforcement und detaillierte Filterung für Sessions, die durch die Firewall hindurch gestartet werden. Öffentlich zugängliche Server schützen sich gegen TCP SYN-Überflutung durch Mechanismen wie z. B. die Verwendung halboffener Verbindungsgrenzwerte an der Firewall. Zur Filterung ist noch anzumerken, dass außer einer Beschränkung des Verkehrs im öffentlich

zugänglichen Segment auf relevante Adressen und Ports auch eine Filterung in Gegenrichtung stattfindet. Wenn ein Angriff einen der öffentlichen Server kompromittiert (durch Umgehung der Firewall und Host-basierten IDS), sollte dieser Server keine Gelegenheit haben, das Netzwerk weiter zu attackieren.

Um solche Angriffe abzuwehren, verhindern spezielle Filter, dass die öffentlichen Server unzulässige Anforderungen an andere Stellen richten. So sollte der Webserver gefiltert werden, damit er keine Anforderungen selbsttätig erzeugen, sondern nur auf Anforderungen von Clients reagieren kann. Dies verhindert, dass ein Hacker nach dem ersten Angriff weitere Programme in das kompromittierte Gerät lädt. Hiermit wird auch dafür gesorgt, dass der Hacker bei der ersten Attacke keine unerwünschten Sessions startet. Ein Beispiel für einen solchen Angriff ist die Erzeugung eines xterm vom Webserver durch die Firewall hindurch zum Rechner des Hackers. Zusätzlich verhindern private VLANs im DMZ-Switch, dass ein kompromittierter öffentlicher Server andere Server im gleichen Segment attackiert. Dieser Datenverkehr wird von der Firewall überhaupt nicht erkannt, was erklärt, warum private VLANs so kritisch sind.

Aus der Host-Perspektive verfügt jeder Host im öffentlich zugänglichen Segment über eine Host-basierte Intrusion-Protection-Software zur Erkennung jeder bösartigen Aktivität auf der Betriebssystem-Ebene sowie von Aktivitäten in gebräuchlichen Server-Applikationen (HTTP, FTP, SMTP, usw.). Der DNS-Host sollte so eingestellt werden, dass er nur auf die gewünschten Befehle reagiert und keine unnötigen Antworten liefert, die Hackern das Ausspionieren des Netzwerks erleichtern können. Hierzu gehört das Verhindern von Bereichstransfers von allen anderen Stellen als den zulässigen sekundären DNS-Servern. Für Maildienste filtert die Firewall selbst die SMTP-Nachrichten in Layer 7, so dass nur zulässige Befehle zum Mailserver gelangen.

Firewalls und Firewall-Router verfügen im Rahmen ihrer Sicherheitsfunktion gewöhnlich über begrenzte NIDS-Fähigkeiten. Diese Fähigkeit wirkt sich zwar auf die Leistungsfähigkeit des Gerätes aus, liefert jedoch zusätzliche Informationen über eventuelle Angriffe. Hier ist also ein Kompromiss zwischen der Leistung und der Erkennung von Angriffen erforderlich. Viele dieser Angriffe können zwar auch ohne den Einsatz der IDS abgewehrt werden, aber in diesem Fall merkt die Überwachungsstation nicht, dass gerade ein bestimmter Angriff stattfindet.

Die VPN-Anbindung erfolgt über die Firewall oder die Firewall/Router-Kombination. Dezentrale Standorte authentifizieren sich untereinander mit Hilfe von vorher ausgetauschten Schlüsseln, und dezentrale Benutzer werden durch den Access Control Server im Campus Modul authentifiziert.

Alternativen

Mögliche Abweichungen von diesem Design würden darauf abzielen, die Kapazität des Netzwerks zu vergrößern oder die verschiedenen Sicherheitsfunktionen auf separate Geräte aufzuteilen. Hierdurch wird das Design dem mittelgroßen Netzwerkdesign immer ähnlicher, das an späterer Stelle in diesem Dokument beschrieben wird. Statt nun das mittelgroße Design komplett zu übernehmen, könnte man als ersten Schritt einen dedizierten VPN-Konzentrator für den Fernzugriff hinzufügen, um das Management der dezentralen Benutzer zu verbessern.

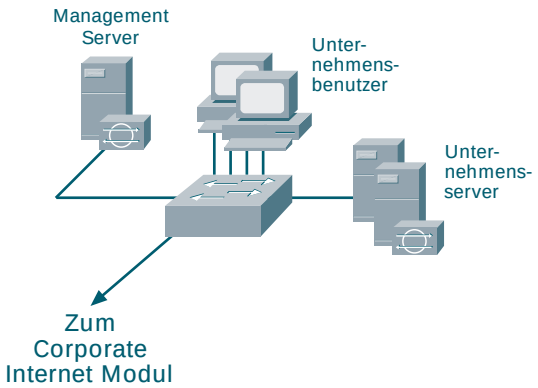
Campus Modul

Das Campus Modul beinhaltet Arbeitsstationen für die Endanwender, Server für die unternehmenseigenen Intranets und das Netzwerkmanagement sowie die dazugehörige Layer-2-Infrastruktur, die zur Geräteunterstützung erforderlich ist. In einem kleinen Netzwerk ist die Layer-2-Funktionalität in einem einzigen Switch zusammengefasst.

Hauptgeräte

- **Layer-2-Switching (mit Unterstützung von privaten VLANs):** Liefert Layer-2-Dienste für alle Arbeitsstationen.
- **Unternehmensserver:** Liefert E-Mail-Dienste (SMTP und POP3) für interne Benutzer sowie die Übertragung von File-, Print- und DNS-Diensten zu den Workstations.
- **Arbeitsplätze der Benutzer:** Liefert Datendienste an autorisierte Benutzer auf dem Netzwerk.
- **Management-Host:** Liefert Managementdienste wie HIDS, syslog, TACACS+/RADIUS (Remote Access Dial-In User Service) sowie allgemeines Konfigurationsmanagement

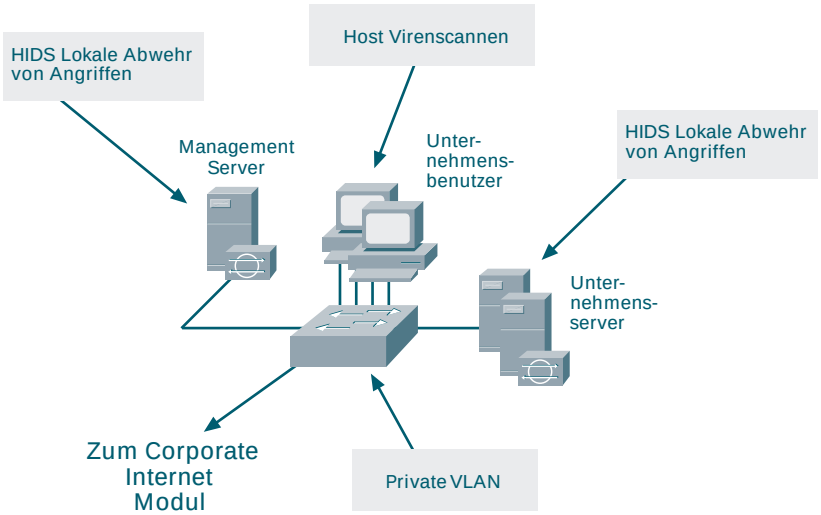
Abbildung 4: Detaillierte Ansicht des Campus Moduls für kleine Netzwerke



Folgende Angriffe werden abgewehrt:

- **Packet Sniffer**: Eine geswitchte Infrastruktur macht Sniffer ineffizient.
- **Viren und trojanische Pferde:** Host-basierte Virenscanner verhindern die Verbreitung von Viren und trojanischen Pferden.
- **Unerlaubter Zugang:** Abwehr von unerlaubtem Zugriff mit Verwendung von host-basierter Angriffserkennung und Zugangskontrollen für Anwendungen.
- **Angriffe in der Anwendungsschicht:** Betriebssysteme, Geräte und Anwendungen werden mit den neuesten Sicherheits-Fehlerkorrekturen auf dem aktuellen Stand gehalten und von HIDS geschützt.
- **Trust Exploitation:** Private VLAN ermöglichen die kontrollierte Kommunikation von Hosts auf einem Subnet
- **Umleitung der Ports:** HIDS verhindert, dass Port Redirection Agents installiert werden.

Abbildung 5: Angriffsabwehr für das Campus Modul in kleineren Netzwerken.



Gestaltungsrichtlinien

Das Campus Modul dient hauptsächlich zum Switchen des Produktions- und Management-Verkehrs und zur Anbindung für die Unternehmens- und Managementserver und Benutzer. Innerhalb des Switch können private VLANs aktiviert werden, um Trust-Exploitation-Angriffe zwischen den Geräten abzuwehren. So kann beispielsweise zugelassen werden, dass die Benutzer im Unternehmen mit den unternehmenseigenen Servern kommunizieren, wobei im Einzelfall jedoch keine Notwendigkeit bestehen muss, dass die Benutzer untereinander kommunizieren.

Da im Campus Modul keine Layer-3-Dienste vorgesehen sind, sollte beachtet werden, dass dieses Design wegen der offenen Auslegung des internen Netzwerkes mehr Wert auf die Sicherheit von Applikationen und Hosts legt. Daher wurde auf wichtigen Systemen innerhalb des Campus auch HIDS installiert, u. a. auf Unternehmensservern und Managementsystemen.

Alternativen

Durch Zwischenschaltung eines kleinen Routers oder einer Firewall mit Filterung zwischen den Management-Stationen und dem übrigen Netzwerk kann man die Sicherheit insgesamt verbessern. Bei dieser Anordnung kann der Management-Verkehr nur in die von den Administratoren vorgegebene Richtung fließen. Wenn innerhalb der Organisation ein hohes Vertrauensniveau herrscht, kann man HIDS wahrscheinlich einsparen; dies wird jedoch nicht empfohlen.

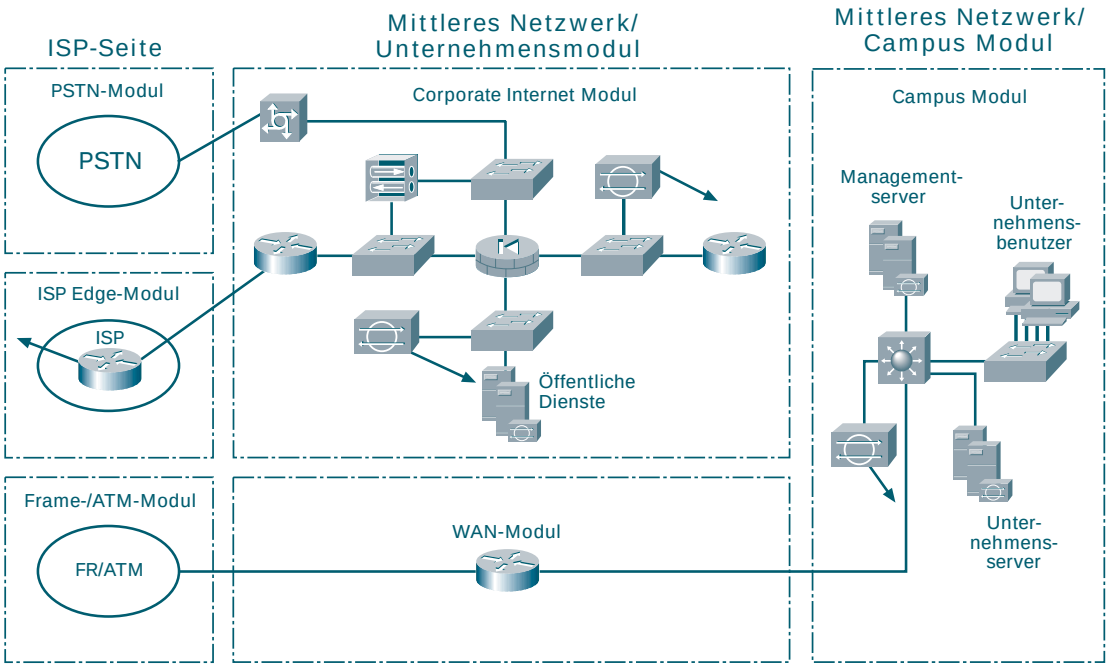
Zweigstellen- oder Standalone-Konfiguration?

Bei der Konfiguration als Zweigstelle ist keine VPN-Funktionalität für den Fernzugriff erforderlich, da dies normalerweise in der Unternehmenszentrale realisiert wird. Die Management-Hosts befinden sich üblicherweise in der Zentrale, wodurch der Management-Verkehr durch die VPN-Verbindung zwischen den Standorten zurück zur Zentrale fließen muss.

Design eines mittelgroßen Netzwerks

Ein SAFE-konformes Netzwerk mittlerer Größe besteht aus drei Modulen: dem Corporate Internet Modul, dem Campus Modul und dem WAN-Modul. Wie beim Design für kleinere Netzwerke stellt das Corporate Internet Modul die Verbindung zum Internet her und terminiert VPN-Verbindungen sowie den Datenverkehr zu öffentlich verfügbaren Netzwerkdiensten wie DNS, HTTP, FTP und SMTP. Der Datenverkehr, der durch Einwahl entsteht, ist ebenfalls am Corporate Internet Modul angeschlossen. Das Campus Modul beinhaltet die Layer-2- sowie Layer-3-Switching-Infrastruktur. Hier sind alle Unternehmensbenutzer, Management- und Intranet-Server angebunden. Für die Anbindung der Remote-User gibt es zwei Möglichkeiten: Entweder eine private WAN-Verbindung unter Verwendung des WAN-Moduls oder eine IPSec VPN-Verbindung zum Corporate Internet Modul. Die meisten Ausführungen zu diesem Design setzen voraus, dass ein Netzwerk mittlerer Größe als Head-End eines Unternehmens eingesetzt wird. Wird es in einer Zweigstelle eingesetzt, wird auf die speziellen Änderungen eingegangen.

Abbildung 6: Detaillierte Ansicht eines mittelgroßen Netzwerks.



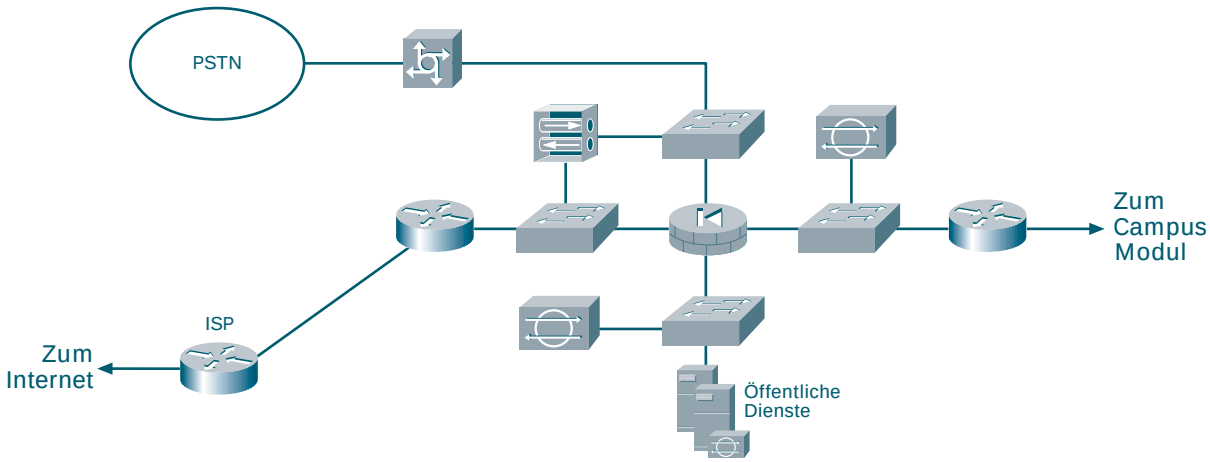
Corporate Internet Modul

Aufgabe des Corporate Internet Moduls ist es, internen Benutzern den Zugang zu Internet-Diensten bereitzustellen und den Internet-Benutzern Zugriff auf Informationen auf öffentlichen Servern zu ermöglichen. Das Modul terminiert zusätzlich Datenverkehr von mobilen Arbeitern und Außenstellen sowie den Datenverkehr von Benutzern, die per Einwahl verbunden sind. Das Corporate Internet Modul ist nicht dafür geeignet, E-Commerce-Anwendungen bereitzustellen. Im Abschnitt „E-Commerce-Modul“ in SAFE Enterprise erhalten Sie mehr Informationen dazu.

Hauptgeräte

- **Einwahlserver:** Authentifiziert individuelle Remote-Users und terminiert deren analoge Wählverbindungen.
- **DNS Server:** Dient als autorisierender externer DNS Server für ein mittelgroßes Netzwerk; reicht interne Anfragen an das Internet weiter.
- **FTP/HTTP Server:** Stellt öffentlich zugängliche Informationen über das Unternehmen bereit.
- **Firewall:** Sorgt für einen Schutz der Ressourcen auf Netzwerkebene mit Stateful-Filtering-Funktionen. Sie stellt differenzierte Sicherheitslösungen für mobile Benutzer zur Verfügung, authentifiziert berechtigte Außenstellen und liefert Konnektivität über IPSec-Tunnel.
- **Layer-2-Switches (mit Unterstützung privater VLAN):** Stellt die Verbindung von Geräten über Layer-2 zur Verfügung.
- **NIDS-Appliance:** Überwacht die Netzwerksegmente auf Layer-4 und Layer-7 innerhalb des Moduls.
- **SMTP Server:** Stellt die Verbindungsstelle zwischen dem Internet und dem Mail Server im Intranet dar und untersucht die Inhalte.
- **VPN Concentrator:** Authentifiziert individuelle mobile Arbeiter und terminiert ihre VPN-Tunnel.
- **Edge Router:** Bietet einfache Filter und Internetverbindungen über Layer-3.

Abbildung 7: Detaillierte Ansicht des Corporate Internet Moduls in einem mittelgroßen Netzwerk.



Folgende Angriffe werden abgewehrt:

Die öffentlich verfügbaren Server sind innerhalb dieses Moduls häufige Angriffsziele. Folgende Gefahren sind zu erwarten:

- **Unautorisierter Zugang:** Wird durch Filterung auf der ISP-Seite, am Edge Router und an der Firewall des Unternehmens verhindert.
- **Angriffe auf der Anwendungsschicht:** Werden durch Einsatz von netzwerk- und host-basierten IDS verhindert.
- **Angriffe durch Viren und trojanische Pferde:** Werden durch Filterung von E-Mail-Inhalten, HIDS und host-basiertes Virenscannen erkannt.
- **Passwort-Angriffe:** Verfügbare Dienste für Brute-Force-Angriffe sind eingeschränkt; Betriebssystem und IDS erkennen die Angriffe.
- **Denial of Service:** Garantierte Zugangsraten (CAR) auf der ISP-Seite und TCP-Intercept auf der Firewall.
- **IP-Spoofing:** Filterung auf ISP-Seite nach RFC 2827 und 1918 und am Zugangsrouter des mittelgroßen Netzwerks.
- **Packet Sniffer:** Die geswitchte Infrastruktur sowie ein host-basiertes IDS limitieren die Einsatzmöglichkeiten.
- **Network Reconnaissance:** IDS erkennen das Ausspionieren des Netzwerks. Geeignete Protokoll-Filter flankieren diese Maßnahme.
- **Trust Exploitation:** Wird durch ein restriktives Trust-Modell sowie den Einsatz von privaten VLAN vermieden.
- **Umleitung von Ports:** Wird durch strenges Filtern und den Einsatz von HIDS verhindert.

Die RAS- und Site-to-Site-VPN-Dienste innerhalb des Moduls können ebenfalls Ziel der folgenden Angriffe werden:

- **Network Topology Discovery:** Filterlisten (Access Control Lists – ACL) auf dem Internet-Router beschränken den Zugriff auf den VPN Concentrator und die Firewall (wenn sie eingesetzt wird, um IPSec-Tunnel von Außenstellen zu terminieren) auf IKE (Internet Key Exchange) und ESP (Encapsulating Security Payload) aus dem Internet
- **Passwort-Angriffe:** Einmal-Passwörter (One-Time Passwords – OTP) verringern die Gefahr von Brute-Force-Angriffen.
- **Unerlaubter Zugang:** Firewall-Dienste nach der Packet-Entschlüsselung verhindern Datenverkehr auf unautorisierten Ports.
- **Man-in-the-middle-Attacken:** Diese Attacken werden durch verschlüsselten Datenverkehr mit den Außenstellen abgewehrt.
- **Packet Sniffer:** Eine geswitchte Infrastruktur limitiert ihre Einsatzmöglichkeiten.

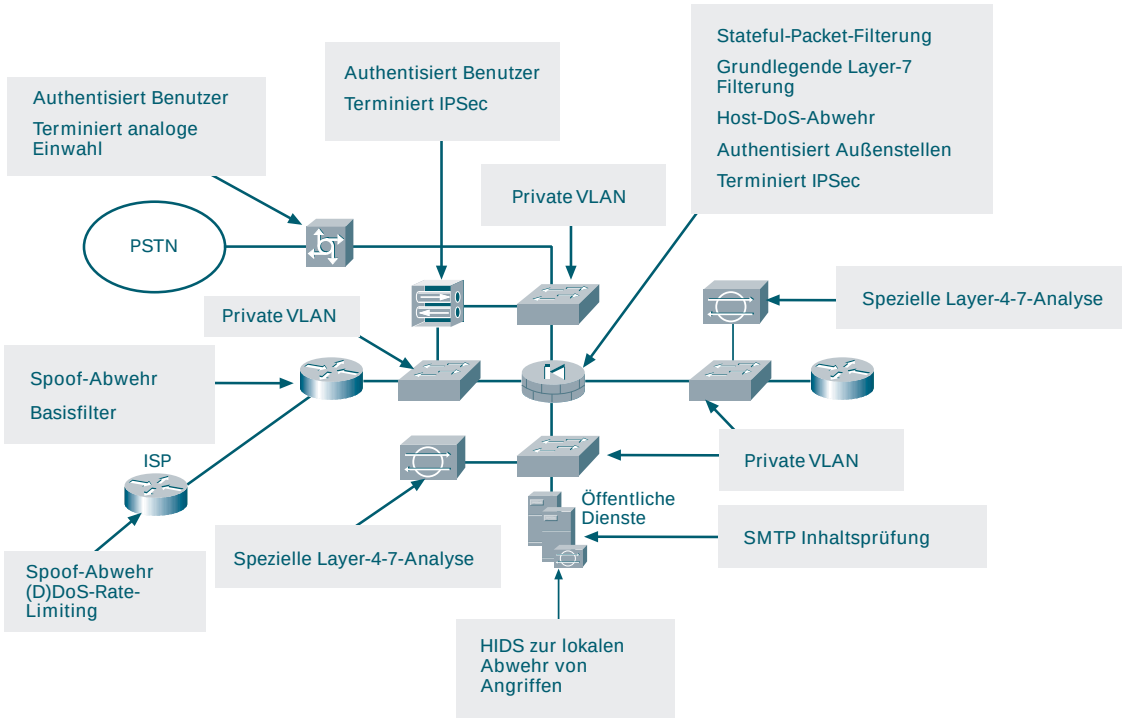


Abbildung 8: Angriffsabwehr für das Corporate Internet Modul in mittelgroßen Netzwerken.

Gestaltungsrichtlinien

Nachfolgend wird die Funktionalität aller Geräte innerhalb des Corporate Internet Moduls beschrieben.

ISP-Router

Der kundenseitige ISP-Router dient hauptsächlich zur Anbindung an das Internet oder das ISP-Netzwerk. Am Ausgang des ISP-Routers erfolgt eine Begrenzung der Übertragungsrate für unerwünschten Datenverkehr, der bestimmte Schwellenwerte überschreitet, wodurch DDoS-Angriffe abgewehrt werden. Ebenfalls am Ausgang des ISP-Routers wehrt eine RFC 1918- und RFC 2827-Filterung das Quelladressen-Spoofing in lokalen Netzwerken und privaten Adressbereichen ab.

Edge-Router

Der Edge-Router im mittelgroßen Netzwerk übernimmt die Abgrenzung zwischen dem ISP-Netzwerk und dem mittelgroßen Netzwerk. Am Eingang des Edge-Routers im mittelgroßen Netzwerk beschränkt eine einfache Filterung den Zugang ausschließlich auf erwarteten IP-Verkehr und bildet damit einen groben Filter für einfache Angriffe. Eine hier ebenfalls vorgesehene RFC 1918- und RFC 2827-Filterung dient zur Verifizierung der ISP-Filterung. Wegen des enormen Sicherheitsrisikos durch fragmentierte Pakete wird der Router zusätzlich so konfiguriert, dass er die meisten fragmentierten Pakete unterdrückt, die für die Standard-Übertragungsarten im Internet nicht typisch sind. Verluste von legalen Datenübertragungen durch diese Filterung werden angesichts des Risikos, das durch Zulassen dieses Datenverkehrs entstehen würde, als akzeptabel angesehen. Der gesamte für den VPN-Konzentrator oder die Firewall bestimmte IPSec-Verkehr wird durchgelassen.

Die Filterung am Router wird so konfiguriert, dass nur IKE- und IPSec-Verkehr den VPN-Konzentrator oder die Firewall erreicht. Bei VPNs für den Fernzugriff ist die IP-Adresse des dezentralen Systems nicht allgemein bekannt, so dass die Filterung nur für den Head-End-Peer (VPN-Konzentrator), mit dem die dezentralen Benutzer kommunizieren, spezifiziert zu werden braucht. Bei den VPNs zwischen den Standorten ist die IP-Adresse des dezentralen Standortes normalerweise bekannt; daher kann eine Filterung für den VPN-Datenverkehr von und zu beiden Peers vorgesehen werden.

Firewall

Die Hauptaufgabe der Firewall ist Connection-State-Enforcement und die detaillierte Filterung für Sessions, die durch die Firewall hindurch gestartet werden. Sie dient auch als Endpunkt für die IPSec VPN-Tunnel zwischen den Standorten für den Produktionsverkehr und den Managementverkehr am dezentralen Standort. Mit der Firewall sind mehrere Segmente verbunden. Das erste ist das Segment mit den öffentlichen Diensten, das alle öffentlich zugänglichen Hosts enthält. Das zweite wird für das Fernzugriffs-VPN und den Einwahlzugriff verwendet, was später erläutert wird.

Öffentlich zugängliche Server schützen sich gegen TCP SYN-Überflutung durch Mechanismen wie z. B. die Verwendung halboffener Verbindungsgrenzwerte an der Firewall. Zur Filterung ist noch anzumerken, dass außer einer Beschränkung des Verkehrs im öffentlich zugänglichen Segment auf relevante Adressen und Ports auch eine Filterung in Gegenrichtung stattfindet. Wenn ein Angriff einen der öffentlichen Server kompromittiert (durch Umgehung der Firewall und Host-basierten IDS), sollte dieser Server keine Gelegenheit haben, das Netzwerk weiter zu attackieren. Um solche Angriffe abzuwehren, verhindern spezielle Filter, dass die öffentlichen Server unzulässige Anforderungen an andere Stellen richten.

So sollte der Webserver gefiltert werden, damit er keine Anforderungen selbsttätig erzeugen, sondern nur auf Anforderungen von Clients reagieren kann. Dies verhindert, dass ein Hacker nach dem ersten Angriff weitere Programme in das kompromittierte Gerät lädt. Hiermit wird auch dafür gesorgt, dass der Hacker bei der ersten Attacke keine unerwünschten Sessions startet. Ein Beispiel für einen solchen Angriff ist die Erzeugung eines xterm vom Webserver durch die Firewall hindurch zum Rechner des Hackers. Zusätzlich verhindern private VLANs im DMZ-Switch, dass ein kompromittierter öffentlicher Server andere Server im gleichen Segment attackiert. Dieser Datenverkehr wird von der Firewall überhaupt nicht erkannt, was erklärt, warum private VLANs so kritisch sind.

Erkennung von Angriffen

Das Segment mit den öffentlich zugänglichen Diensten ist mit einem NIDS-Gerät ausgestattet. Dieses soll vor allem Angriffe auf Ports erkennen, welche die Firewall aufgrund ihrer Konfiguration zulässt. Hierbei handelt es sich vorwiegend um Application Layer-Angriffe auf bestimmte Dienste. Das NIDS im Segment mit den öffentlich zugänglichen Diensten sollte restriktiv konfiguriert werden, da die hier anerkannten Signaturen bereits die Firewall ohne Beanstandung passiert haben. Jeder Server ist auch mit einem HIDS ausgestattet. Das HIDS dient hauptsächlich zur Erkennung jeder bösartigen Aktivität auf der Betriebssystem-Ebene sowie von Aktivitäten in gebräuchlichen Server-Applikationen (HTTP, FTP, SMTP, usw.).

Der DNS sollte so eingestellt werden, dass er nur auf die gewünschten Befehle reagiert und keine unnötigen Antworten liefert, die Hackern das Ausspionieren des Netzwerks erleichtern können. Hierzu gehört das Verhindern von Bereichstransfers von allen anderen Stellen als den zulässigen sekundären DNS-Servern. Der SMTP-Server verfügt über Prüffunktionen für Mail-Inhalte, die Angriffe auf das interne Netzwerk mit Viren und Trojanischen Pferden abwehrt, die gewöhnlich über das Mail-System erfolgen. Die Firewall selbst filtert SMTP-Nachrichten in Layer 7, um nur die nötigen Befehle an den Mailserver weiterzugeben.

Das NIDS-Gerät zwischen der privaten Schnittstelle der Firewall und dem internen Router führt eine letzte Analyse von Angriffen durch. In diesem Segment sollten nur noch sehr wenige Angriffe erkannt werden, da nur Antworten auf initiierte Anfragen, einige ausgewählte Ports des öffentlich zugänglichen Segmentes und Datenverkehr aus dem Fernzugriffs-Segment bis ins Innere durchgelassen werden. Bis in dieses Segment sollten nur noch sehr komplexe Angriffe durchkommen, denn dies würde bedeuten, dass ein System im öffentlichen Segment kompromittiert wurde und der Hacker versucht, dieses als Ausgangspunkt für einen Angriff auf das interne Netzwerk zu nutzen. Wurde beispielsweise der öffentliche SMTP-Server kompromittiert, kann ein Hacker versuchen, über den TCP-Port 25 in den internen Mailserver einzudringen, der Mail-Transfers zwischen den beiden Hosts durchführen darf. Wenn in diesem Segment Angriffe festgestellt werden, so sollte die Antwort darauf deutlicher als in den anderen Segmenten ausfallen, da diese auf eine bereits erfolgte Sicherheitsverletzung hindeuten. Die Verwendung von TCP-Resets oder Shunning-Funktionen zur Abwehr von Vorkommnissen wie der oben beschriebenen SMTP-Attacke sollte ernsthaft in Erwägung gezogen werden.

VPN für Fernzugriff

Der VPN-Konzentrator für den Fernzugriff dient vor allem zur sicheren Anbindung von dezentralen Benutzern an das mittelgroße Netzwerk. Der VPN-Konzentrator startet eine Session mit einem Access Control Server im internen Netzwerk, um die Benutzer zu authentifizieren, bevor sie Zugang zum Netzwerk erhalten. Der Access Control Server sendet anschließend eine Anfrage an ein OTP (One-Time Passwort)-System, um die Authentifizierungsangaben des Benutzers zu verifizieren. Über eine vom Konzentrator an den Client geschickte IPSec Policy wird verhindert, dass die Benutzer eine Split-Tunnelling-Session starten; damit werden die Benutzer gezwungen, über den Unternehmensanschluss auf das Internet zuzugreifen. Die IPSec-Parameter verwenden den Triple Data Encryption Standard (3DES) für die Verschlüsselung und einen sicheren Hash-Algorithmus/Hash-basierten Authentifizierungscode (SHA/HMAC) für die Datenintegrität. Bei Beendigung des VPN-Tunnels wird der Datenverkehr durch eine Firewall geleitet, um eine angemessene Filterung für die VPN-Benutzer sicherzustellen. Diese Anordnung ermöglicht auch das IDS-Shunning in der Firewall. Dieses Szenario steht im Gegensatz zu vielen anderen bestehenden Systemen, bei denen die Firewall vor dem VPN-Gerät angeordnet ist. Die vorgeschaltete Anordnung hat jedoch den Nachteil, dass die Art des Benutzer-Datenverkehrs nicht feststellbar ist, da dieser noch verschlüsselt ist.

Benutzer mit Einwahlzugang

Die herkömmlichen Benutzer mit Einwahlzugang werden an einem Zugangsrouter mit eingebauten Modems terminiert. Wenn die Layer 2-Verbindung zwischen Benutzer und Server aufgebaut wurde, wird der Benutzer mit Hilfe des CHAP (Challenge Handshake Authentication Protocol)-Dreiwegeprotokolls authentifiziert. Wie beim VPN-Dienst für den Fernzugriff wird zur Authentifizierung der AAA (Authentification, Authorization and Accounting)-Server verwendet. Nach erfolgter Authentifizierung erhalten die Benutzer IP-Adressen aus einem IP-Pool.

Layer 2-Switches

Die Switches im Corporate Internet Modul dienen hauptsächlich zur Layer 2-Anbindung zwischen den verschiedenen Geräten innerhalb des Moduls. Statt eines einzigen Switches mit mehreren VLANs werden einzelne Switches verwendet, um eine physikalische Trennung zwischen dem äußeren Segment, dem Segment mit den öffentlich zugänglichen Diensten, dem VPN-Segment und dem inneren Segment zu realisieren. Diese Anordnung schützt vor möglichen fehlerhaften Konfigurationen eines Switch, durch welche die Sicherheit in Frage gestellt werden kann. Zusätzlich ist auf jedem Switch die private VLAN-Funktion implementiert, was zur Abwehr von Angriffen durch Trust Exploitation beiträgt.

Innerer Router

Der innere Router dient hauptsächlich zur Layer 3-Trennung und zum Routing zwischen dem Corporate Internet Modul und dem Campus Modul. Dieses Gerät funktioniert ausschließlich als Router ohne Zugangslisten zur Einschränkung des Datenverkehrs über jede Schnittstelle. Da die Routing-Information selbst bei einem DoS-Angriff benutzt werden kann, können solche Angriffe durch Authentifizierung von Routing-Updates zwischen den Geräten abgewehrt werden. Dieser Router stellt die letzte Abgrenzung zwischen dem Routed-Intranet und der Außenwelt dar. Da die meisten Firewalls ohne Routing-Protokolle konfiguriert werden, muss man im Corporate Internet Modul einen Routing-Punkt bereitstellen, der nicht vom Rest des Netzwerks abhängig ist.

Alternativen

Für dieses Modul gibt es mehrere Design-Alternativen. Statt eine einfache Filterung im Edge-Router zum mittelgroßen Netzwerk vorzusehen, kann der Netzwerkadministrator auf diesem Gerät auch eine Stateful-Firewall implementieren. Zwei Stateful-Firewalls bieten einen tiefer gehenden Schutz innerhalb des Moduls. Je nachdem, ob der Netzwerkadministrator eine Benachrichtigung bei einem Angriff wünscht, kann vor der Firewall ein NIDS-Gerät erforderlich sein. Mit den entsprechenden einfachen Filtern kann das IDS außerhalb der Firewall wichtige Alarm-Informationen liefern, die andernfalls von der Firewall unterdrückt würden. Wahrscheinlich entstehen in diesem Segment zahlreiche Alarm-Meldungen, so dass die hier erzeugten Alarme weniger gravierend sein dürften als die hinter einer Firewall ausgelösten Alarme.

Zusätzlich ist eine Protokollierung der aus diesem Segment kommenden Alarme auf einer separaten Management-Station in Betracht zu ziehen, damit begründete Alarme aus anderen Segmenten die nötige Aufmerksamkeit erhalten. Mit der Benachrichtigungsfunktion dieses NIDS außerhalb der Firewall kann besser festgestellt werden, welcher

Art von Angriffen das Unternehmen ausgesetzt ist. Darüber hinaus kann der Wirkungsgrad von Edge-Filtern beim ISP und im Unternehmen untersucht werden.

Zwei weitere Alternativen stehen zur Verfügung. Bei der ersten entfällt der Router zwischen der Firewall und dem Campus Modul. Dessen Funktionen können zwar in den Layer 3-Switch des Campus Moduls integriert werden, jedoch entfällt bei dieser Anordnung die Möglichkeit, das Corporate Internet Modul ohne Layer 3-Dienste aus einem anderen Bereich des Netzwerks zu betreiben. Bei der zweiten Alternative wird zusätzlich zu der bereits vorgesehenen Überprüfung der Mail-Inhalte eine weitere inhaltliche Überprüfung eingefügt. So könnte man beispielsweise einen Server mit URL-Filterung in dem Segment mit den öffentlich zugänglichen Diensten vorsehen um zu regeln, auf welche Arten von Webseiten die Mitarbeiter zugreifen können.

Campus Modul

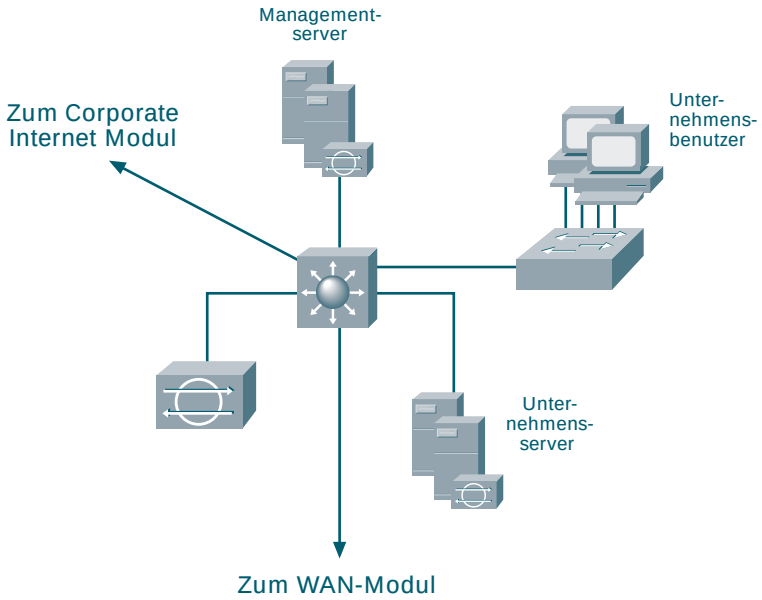
Das Campus Modul besteht aus den Arbeitsstationen, unternehmenseigenen Intranet-Servern, Managementservern und der angeschlossenen Layer-2- und Layer-3-Infrastruktur, mit der die Geräte unterstützt werden. Alle Campus Module aus SAFE Enterprise wurden in einem einzigen Modul zusammengefasst, um den Anforderungen mittelgroßer Netzwerke besser zu entsprechen und die Gesamtkosten für das Design zu senken.

Wie im Corporate Internet Modul werden die Redundanzfunktionen aus SAFE Enterprise nicht im Design für mittelgroße Netzwerke berücksichtigt.

Hauptgeräte

- **Layer-3-Switch:** Der Datenverkehr aus dem Produktions- und Managementbereich wird innerhalb des Campus Moduls geroutet und geswitcht. Der Switch liefert auf der Verteilungsebene Dienste für die Etagenswitche und setzt Filterregeln um.
- **Layer-2-Switche (mit Unterstützung von privaten VLAN):** Liefern Layer-2-Dienste für Arbeitsstationen.
- **Unternehmensserver:** Liefert E-Mail-Dienste (SMTP und POP3) für die internen Benutzer und Datei-, Druck- und DNS-Dienste für die Arbeitsstationen.
- **Arbeitsstationen:** Liefern Dateidienste an autorisierte Benutzer im Netzwerk.
- **SNMP-Management:** Stellt Management-Dienste für SNMP-fähige Geräte zur Verfügung.
- **NIDS Host:** Stellt die zentrale Darstellung der Alarme für alle NIDS-Geräte im Netzwerk zur Verfügung.
- **Syslog Host(s):** Sammelt die Log-Informationen der Firewalls und NIDS-Hosts und wertet sie aus.
- **Server zur Zugangskontrolle:** Liefert den Netzwerkgeräten Authentifizierungsdienste.
- **OTP-Server (One Time Password):** Autorisiert einmalige Passwörter, die vom Zugangskontroll-Server angefragt werden.
- **Systemverwaltungshost:** Liefert Informationen über Konfiguration und Änderungen an Software und Inhalten für die Geräte.
- **NIDS-Appliance:** Liefert die Überwachung der wichtigsten Netzwerksegmente auf Layer-4 und Layer-7.

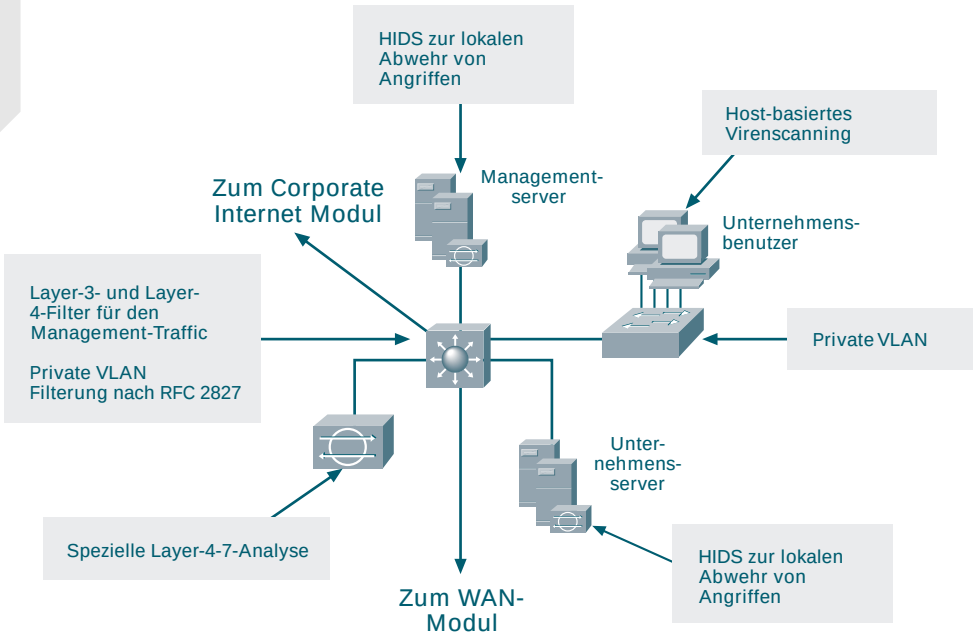
Abbildung 9: Detaillierte Ansicht des Campus Moduls in mittelgroßen Netzwerken.



Folgende Angriffe werden abgewehrt:

- **Packet Sniffer:** Eine geswitchte Infrastruktur macht Sniffer uneffektiv.
- **Viren und trojanische Pferde:** Host-basierte Virenscanner erkennen die meisten Viren und trojanischen Pferde.
- **Unautorisierter Zugang:** Angriffe werden mit dem Einsatz von HIDS und Zugangskontrollen abgewehrt.
- **Passwort-Angriffe:** Der Zugangskontroll-Server bietet Authentifizierung der wichtigsten Anwendungen über zwei Faktoren.
- **Angriffe auf der Verteilungsschicht:** Betriebssysteme, Geräte und Anwendungen werden mit den neusten Fehlerkorrekturen auf dem aktuellsten Stand gehalten und von HIDS geschützt.
- **IP-Spoofing:** Filterung nach RFC 2827 verhindert das Spoofing von Herkunftsadressen.
- **Trust Exploitation:** Die Trust-Modelle sind sehr detailliert; private VLAN verhindern, dass Hosts auf dem Subnet miteinander kommunizieren, wenn dies nicht erforderlich ist.
- **Umleitung der Ports:** HIDS verhindert, dass Port Redirection Agents installiert werden.

Abbildung 10: Angriffsabwehr im Campus Modul für mittelgroße Netzwerke.



Gestaltungsrichtlinien

Nachfolgend wird die Funktionalität der einzelnen Geräte im Campus Modul beschrieben.

Kern-Switch

Die Hauptfunktionen des Kern-Switches sind Routing- und Switching-Funktionen für den Produktions- und Management-Datenverkehr, die Distribution Layer-Dienste (Routing, Quality of Service [QoS] und Zugangskontrolle) für die Etagen-Switches, die Anbindung von Unternehmens- und Managementservern und weitergehende Dienste wie die Verkehrsfilterung zwischen den Teilnetzen. Anstelle eines Layer 2-Switches wird ein Layer 3-Switch verwendet, um getrennte VLANs für das/die Corporate Server Segment(e), das Management Server Segment, das/die Corporate User Segment(e) und die Anbindung an das WAN-Modul und an das Corporate Internet Modul zu realisieren. Der Layer 3-Switch bildet eine Verteidigungslinie zur Abwehr von Angriffen von innen. Er kann durch Zugangskontrolle verhindern, dass eine Abteilung auf vertrauliche Informationen auf dem Server einer anderen Abteilung zugreift. So kann man beispielsweise in einem Netzwerk, das die Bereiche Marketing sowie Forschung und Entwicklung umfasst, den FuE-Server in einem eigenen VLAN abtrennen und den Zugang hierzu durch ein Filter steuern, so dass nur FuE-Mitarbeiter einen Zugriff erhalten. Aus Leistungsgründen muss diese Zugangskontrolle auf einer Hardware-Plattform implementiert werden, die gefilterten Netzwerkverkehr mit nahezu der maximalen Leitungsgeschwindigkeit bereitstellen kann. Diese Konfiguration erfordert im allgemeinen die Verwendung von Level 3-Switching anstelle der herkömmlichen dedizierten Routing-Geräte. Die gleiche Zugangskontrolle kann durch RFC 2827-Filterung auch das Spoofing lokaler Quelladressen verhindern. Eine RFC 2827-Filterung sollte auf den Corporate User- und Corporate Intranet Server-VLANs eingerichtet werden.

Innerhalb jedes VLANs können private VLANs eingerichtet werden, um Trust Exploitation-Angriffe zwischen den Geräten zu verhindern. So kann es beispielsweise nicht erforderlich sein, dass die einzelnen Server innerhalb des Corporate Server Segmentes miteinander kommunizieren. Sie müssen nur mit den an das/die Corporate User Segment(e) angeschlossenen Geräte kommunizieren können.

Zum Aufbau einer weiteren Verteidigungslinie für die Management-Server wird eine umfangreiche Layer 3- und Layer 4-Filterung am Ausgang der VLAN-Schnittstelle zum Management Server Segment konfiguriert. Der ACL beschränkt den Zugang zu und von den Management-Servern auf die von diesen jeweils gesteuerten Geräte (über die IP-Adresse) und nur für die benötigten Protokolle/Dienste (über Port-Nummer). Dies umfasst auch die Zugangskontrolle für den an die Geräte des dezentralen Standortes gerichteten Management-Verkehr. Dieser Datenverkehr wird von der Firewall verschlüsselt und an die dezentralen Standorte weitergeleitet. Der Zugriff auf die Managed-Geräte wird außerdem dadurch kontrolliert, dass nur bestehende Verbindungen zurück durch den ACL zulässig sind.

Etagen-Switches

Die Hauptaufgabe der Etagen-Switches innerhalb des Campus Moduls ist die Bereitstellung von Layer 2-Diensten für Corporate User-Arbeitsplätze. Zum Schutz gegen Trust Exploitation-Angriffe sind Private VLANs in den Etagen-Switches implementiert, da die einzelnen Endanwender-Arbeitsplätze normalerweise nicht miteinander kommunizieren müssen. Zusätzlich zu den Richtlinien für die Netzwerksicherheit, die in der Sicherheitsrichtline der Switches festgeschrieben sind, ist auf Arbeitsplatz-Ebene auch ein Host-basierter Virenscanner implementiert.

Erkennen von Angriffen

Das Campus Modul enthält ebenfalls ein NIDS-Gerät. Der Switch-Port zum Anschluss an das NIDS-Gerät wird so konfiguriert, dass der Datenverkehr von allen zu überwachenden VLANs an den Überwachungs-Port des NIDS-Gerätes gespiegelt wird. Hier sollten nur sehr wenige Angriffe erkannt werden, da dieses NIDS-Gerät eine Analysefunktion für Angriffe bietet, die aus dem Campus Modul selbst stammen. Wenn beispielsweise eine Benutzer-Workstation durch eine unbekannte Modemverbindung zu diesem Host kompromittiert wurde, kann das NIDS-Gerät verdächtige Aktivitäten erkennen, die aus dem Campus kommen. Andere interne Angriffe können von verärgerten Mitarbeitern stammen, von unbeaufsichtigt gebliebenen und von anderen Personen missbräuchlich benutzten Workstations, oder durch Trojanische Pferde, die versehentlich auf portable PCs geladen wurden. Auf allen Corporate Intranet- und Management-Servern ist außerdem HIDS installiert.

Alternativen

Wenn das mittelgroße Netzwerk klein genug ist, kann man die Funktionalität der Etagen-Switches mit in den Kern-Switch integrieren und die Etagen-Switches einsparen. In diesem Fall wird die Endanwender-Workstation direkt an den Kern-Switch angeschlossen. Private VLAN-Funktionen zur Abwehr von Trust Exploitation-Angriffen werden im Kern-Switch implementiert. Wenn das interne Netzwerk keine hohen Leistungsanforderungen stellt, kann statt des leistungsfähigeren Layer 3-Switch ein separater Router und Layer 2-Switch für den Kern und die Weitergabe verwendet werden.

Auf Wunsch kann man das separate NIDS-Gerät durch ein in den Kern-Switch integriertes IDS-Modul ersetzen. Diese Konfiguration erzeugt einen höheren Verkehrsdurchsatz in das IDS-Modul, da dieses auf der Switch-Backplane angeordnet ist und nicht über einen einzelnen 10/100 MBit/s Ethernet-Port angeschlossen ist. Mit einem ACLs im Switch kann man den zum IDS-Modul weitergeleiteten Datenverkehr steuern.

WAN-Modul

Das WAN-Modul wird verwendet, wenn Außenstellen über private Netzwerke angeschlossen werden. Dies ist der Fall, wenn strenge QoS-Anforderungen über ein IPSec VPN nicht erfüllt werden können oder wenn die vorhandenen WAN-Verbindungen genutzt werden, für die eine Migration auf IPSec zu hohe Kosten verursacht.

Abbildung 11: Detaillierte Ansicht des WAN-Moduls für mittelgroße Netzwerke.

Hauptgeräte

- **IOS-Router**: Stellt Mechanismen für Routing, Zugangskontrolle und QoS für die Außenstellen zur Verfügung.

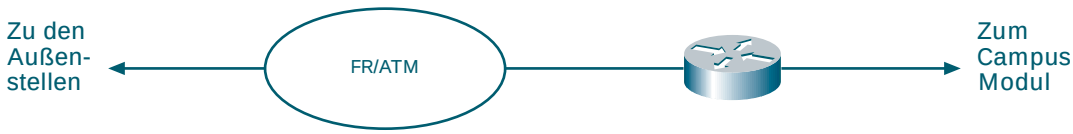
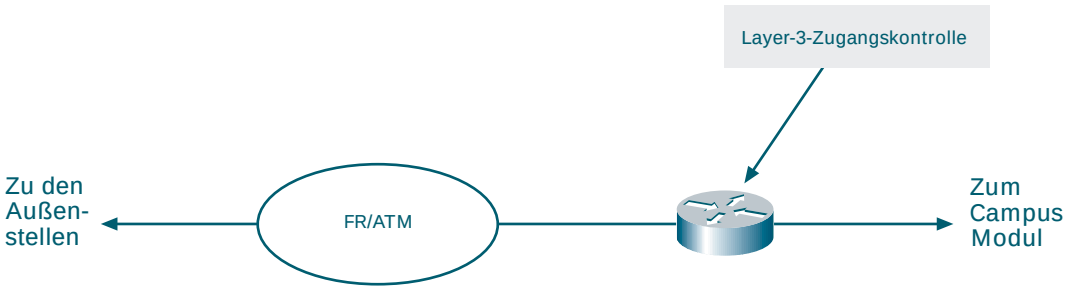


Abbildung 12: Angriffsabwehr für WAN-Module.

Folgende Angriffe werden abgewehrt:

- **IP-Spoofing**: IP-Spoofing wird durch Layer-3-Filterung verhindert.
- **Unautorisierter Zugang:** Einfache Zugangskontrolle auf dem Router schränkt die Zahl der Protokolle ein, auf die die Zweigstellen Zugang haben.



Gestaltungsrichtlinien

Der Grad der im WAN-Modul realisierten Sicherheit richtet sich nach dem Grad des Vertrauens für die dezentralen Standorte und für den ISP, an den das Netzwerk angebunden ist. Die Sicherheit wird durch den Einsatz von IOS-Funktionen realisiert. In diesem Netzwerkdesign wird jeglicher ankommender unerwünschter Datenverkehr mit Hilfe von Zugangslisten an der seriellen Schnittstelle daran gehindert, in das mittelgroße Netzwerk zu gelangen. Mit Zugangslisten für den ankommenden Datenverkehr an der Ethernet-Schnittstelle kann der vom mittelgroßen Netzwerk an die dezentralen Standorte zurückfließende Verkehr weiter eingeschränkt werden.

Alternativen

Organisationen, die um die vertrauliche Behandlung ihrer Informationen sehr besorgt sind, verschlüsseln den Datenverkehr auf ihren klassischen WAN-Verbindungen. Dieser Vertraulichkeitsgrad kann wie beim Datenverkehr zwischen verschiedenen Standorten mit IPSec erzielt werden. Der Einsatz einer Firewall im WAN-Router bietet weitergehende Möglichkeiten für die Zugangskontrolle über die im SAFE-Design verwendete grundlegende ACL-Funktionalität hinaus.

Zweigstellen- oder Head-End-Design?

Bei der Konfiguration als Zweigstelle können mehrere Komponenten im mittelgroßen Netzwerk eingespart werden. Die erste Überlegung ist, ob eine Organisation über eine private WAN-Verbindung oder ein IPSec VPN an die Unternehmenszentrale angeschlossen werden soll. Zu den Argumenten für das private WAN zählen eine feiner abgestufte QoS-Unterstützung, Multicast-Support, Zuverlässigkeit der Netzwerk-Infrastruktur oder die Notwendigkeit für Nicht-IP-Übertragungen. Hierbei ist zu beachten, dass bei Verwendung von IPsec über GRE (Generic Routing Encapsulation) (siehe SAFE Enterprise) Multicast- und Nicht-IP-Übertragungen in einer VPN-Umgebung unterstützt werden. Mehrere Gründe sprechen für IPSec VPNs anstelle einer privaten WAN-Verbindung. Zunächst einmal kann ein IPSec VPN im Internet den lokalen Internetzugang für alle dezentralen Standorte realisieren, wodurch man im Head-End-Bereich Bandbreite (und Kosten) einsparen kann. In vielen nationalen und den meisten internationalen Anwendungen bieten IPSec VPNs erhebliche Kostenvorteile gegenüber privaten WAN-Verbindungen.

Wenn eine private WAN-Verbindung für das mittelgroße Netzwerk in einer Zweigstellen-Konfiguration verwendet wird, wird das gesamte Corporate Internet Modul nicht benötigt (sofern kein lokaler Internetzugang von der Zweigstelle aus erforderlich ist). Umgekehrt wird bei Verwendung des IPSec VPN das WAN-Modul nicht benötigt. Außer dem WAN-Modul braucht ein mittelgroßes Zweigstellen-Design unter Umständen keinen VPN-Konzentrator oder Einwahl-Router für den dezentralen Zugriff, wenn diese Dienste von der Unternehmenszentrale zur Verfügung gestellt werden.

Aus der Management-Perspektive lässt sich feststellen, dass Konfigurieren und Sicherheitsmanagement des mittelgroßen Netzwerkes vom Management-Modul der Unternehmenszentrale übernommen werden (unter der Voraussetzung zentraler IT-Ressourcen). Wenn zur Verknüpfung der Standorte eine private WAN-Verbindung verwendet wird, kann der Management-Verkehr problemlos über das WAN-Modul zu den Geräten fließen, die Management-Aktivitäten erfordern.

Wird die Verbindung zwischen den Standorten mit einem IPSec VPN hergestellt, kann der meiste Management-Verkehr in der gleichen Weise wie bei Verwendung einer privaten WAN-Verbindung fließen. Einige Einrichtungen, z. B. der Edge-Router außerhalb der Firewall, ist dann kein Teil des IPSec Tunnels und muss auf andere Weise verwaltet werden. Diese Konfiguration könnte einen separaten IPSec Tunnel zum Gerät vorsehen oder Konfigurationsänderungen für diese Geräte mittels Application Layer-Verschlüsselung (SSH) vornehmen. Wie bereits in den Grundsätzen erwähnt, gibt es nicht für alle Management-Protokolle eine entsprechende sichere Variante.

Design für mobile Benutzer

In diesem Abschnitt werden vier SAFE-konforme Möglichkeiten vorgestellt, mobile Benutzer und Angestellte im Home Office an das Unternehmensnetzwerk anzubinden. Wichtigste Aufgabe dieses Designs ist die Anbindung der Außenstelle an das Unternehmen und das Internet. Die Möglichkeiten basieren auf reinen Software- oder Hardware-Lösungen oder einer Kombination aus beiden:

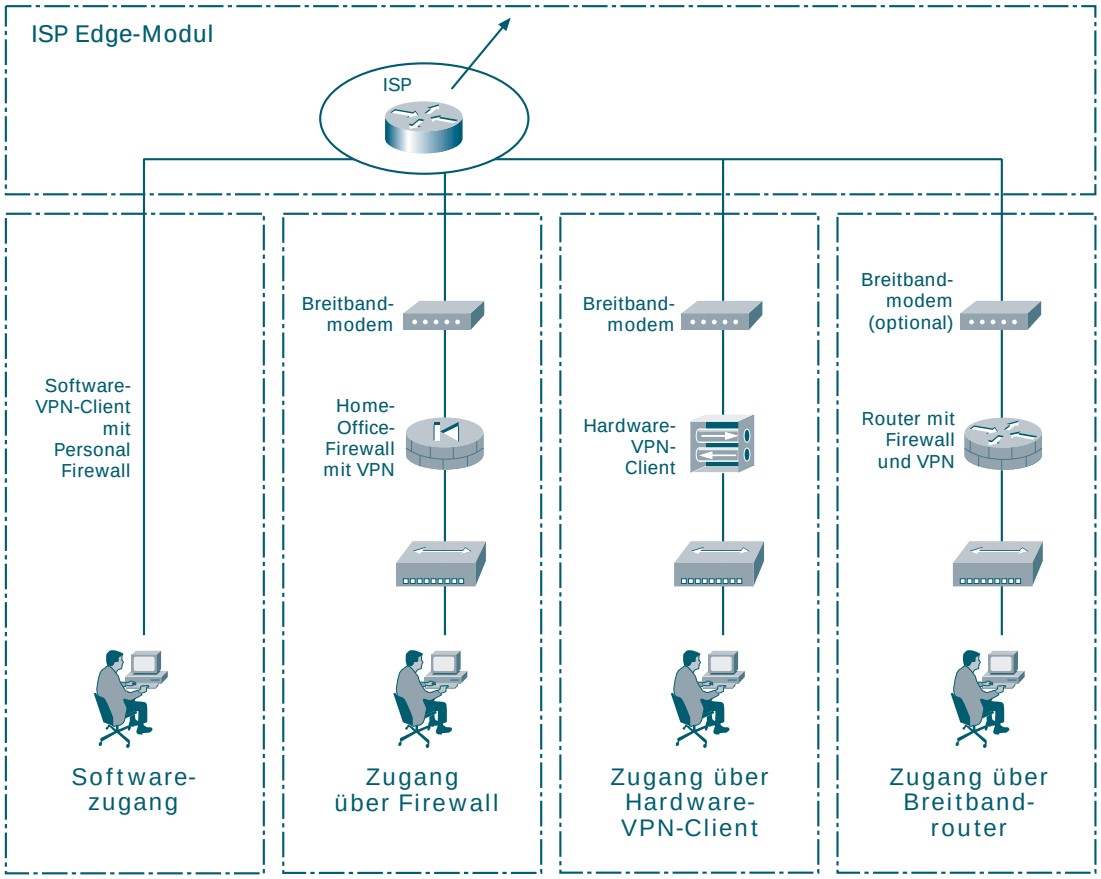
- **Softwarezugang:** Die mobilen Benutzer haben einen VPN-Software-Client und eine Personal Firewall auf ihren PCs installiert.
- **Zugang über eine externe Firewall:** Die Arbeitsstation wird durch eine dezidierte Firewall geschützt und mit einem IPSec-Tunnel per VPN an das Unternehmen angebunden. Die WAN-Verbindung wird über einen Breitbandzugang (beispielsweise Kabel oder xDSL) hergestellt.
- **Zugang über einen Hardware-VPN-Client:** Die Außenstelle nutzt einen dezidierten Hardware-VPN-Client, der die IPSec-VPN-Verbindung zum Unternehmen herstellt. Die WAN-Verbindung wird über einen Breitbandzugang hergestellt.
- **Zugang über einen Router:** Die Außenstelle nutzt einen Router, der eine IPSec-VPN-Verbindung zum Unternehmen herstellt. Der Router kann entweder einen direkten Zugang zum Breitbandnetz herstellen oder an ein Breitbandmodem angeschlossen werden.

Alle Designs werden im folgenden genauer beschrieben. Bei allen dargestellten Verbindungen wird davon ausgegangen, dass die Verbindung über das Internet hergestellt wird. Wenn private WAN-Verbindungen (ISDN, privates DSL usw.) genutzt werden, ist eine Verschlüsselung des Datenverkehrs nicht unbedingt notwendig. Für jede der oben genannten Möglichkeiten sollte der Sicherheitsbereich eines Unternehmens auf die Außenstellen vergrößert werden.

Hauptgeräte

- **Breitbandmodem: S**tellt den Zugang zum Breitbandnetz her (DSL, Kabel etc.).
- **Firewall mit VPN-Unterstützung:** Stellt sichere und verschlüsselte Ende-zu-Ende-Tunnel von der Außenstelle zum Head-End des Unternehmensnetzwerks her. Sie schützt die Ressourcen der Außenstelle auf Netzwerkebene und liefert Stateful-Filterung des Datenverkehrs.
- **Layer-2-Hub:** Verbindet die Geräte in der Außenstelle und kann in die Firewall oder den Hardware-VPN-Client integriert werden.
- **Personal Firewall:** Sichert die einzelnen PCs auf Geräteebene.
- **Router mit Firewall- und VPN-Funktion:** Stellt sichere Ende-zu-Ende-Tunnel zwischen der Außenstelle und dem Head-End im Unternehmensnetzwerk her. Er schützt die Ressourcen der Außenstelle auf Netzwerkebene und liefert Stateful-Filterung des Datenverkehrs. Zusätzlich stellt er erweiterte Dienste wie Sprache oder QoS zur Verfügung.
- **Software-VPN-Client:** Stellt sichere Ende-zu-Ende-Tunnel zwischen den einzelnen PCs und dem Head-End im Unternehmensnetzwerk her.
- **Hardware-VPN-Client:** Stellt sichere Ende-zu-Ende-Tunnel zwischen der Außenstelle und dem Head-End im Unternehmensnetzwerk her.

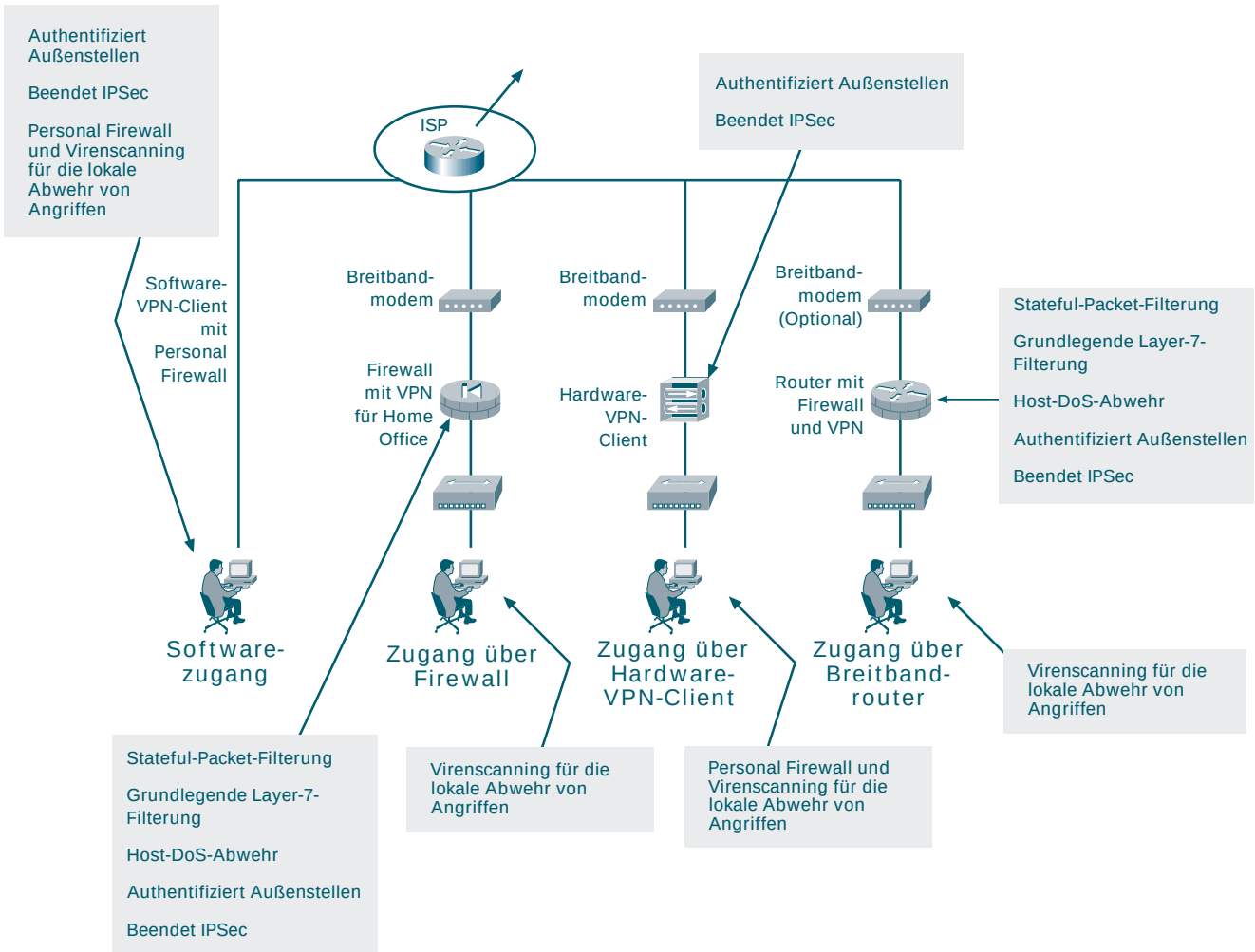
Abbildung 13: Detaillierte Ansicht der Konfiguration für mobile Benutzer.



Folgende Angriffe werden abgewehrt:

- **Unautorisierter Zugang:** Wird durch die Filter- und Stateful-Inspection-Funktionen von Firewall oder Router-Firewall bzw. durch Zugangskontrollen der Personal Firewalls verhindert.
- **Network Reconnaissance:** Protokoll-Filterung auf den Geräten der mobilen Benutzer verhindert, dass ihr Netzwerk ausspioniert werden kann.
- **Angriffe von Viren und trojanischen Pferden:** Wirksamer Virenschutz durch Scanning auf der Hostebene.
- **IP-Spoofing:** Wird durch Filterung nach RFC 2827 und 1918 auf der ISP-Seite verhindert.
- **Man-in-the-middle-Attacken:** Werden durch verschlüsselten Datenverkehr mit den Außenstellen verhindert.

Abbildung 14: Angriffsabwehr im Design für mobile Benutzer.



Gestaltungsrichtlinien

Nachfolgend wird die Funktionalität aller Möglichkeiten für die Anbindung dezentraler Benutzer beschrieben.

Software-Zugang

Der Software-Zugang eignet sich besonders für mobile Benutzer und Heimarbeiter. Diese Benutzer benötigen lediglich einen PC mit VPN Client-Software und einen Zugang zum Internet oder zum ISP-Netzwerk über eine Einwahl- oder Ethernet-Verbindung. Der VPN Software-Client dient in erster Linie zum Aufbau eines sicheren, verschlüsselten Tunnels vom Client-Gerät zu einem VPN Head-End-Gerät. Zugang und Autorisierung für das Netzwerk werden von der Zentrale aus gesteuert; eine Filterung findet an der Firewall und auf dem Client selbst statt, wenn die Zugangsrechte per ‚policy push' übermittelt werden. Der dezentrale Benutzer wird zunächst authentifiziert und erhält anschließend IP-Parameter, u. a. eine virtuelle IP-Adresse für alle VPN Übertragungen und die Adresse der Name Servers (DNS und Windows Internet Name Service [WINS]). Split Tunnelling kann ebenfalls zentral aktiviert oder deaktiviert werden. Für das SAFE-Design wurde das Split Tunnelling ausgeschaltet, hierdurch müssen alle dezentralen Benutzer bei etablierten VPN Tunnel über den Unternehmensanschluss auf das Internet zugreifen. Da der dezentrale Benutzer den VPN Tunnel beim Anschluss an das Internet oder an das ISP-Netzwerk nicht immer aktiviert lassen will, wird die Verwendung einer individuellen Firewall-Software empfohlen, um den PC vor unberechtigten Zugriffen zu schützen. Gegen eine Infektion des PCs mit Viren und Trojanischen Pferden wird die Verwendung eines Virenscan-Programms empfohlen.

Zugang über externe Firewall

Die externe Firewall eignet sich besonders für Heimarbeiter oder auch sehr kleine Zweigstellen. Hierbei wird vorausgesetzt, dass der dezentrale Standort über irgendeinen Breitbandzugang eines Service Providers verfügt. Die Firewall wird nach dem DSL- oder Kabelmodem installiert.

Die Firewall soll vor allem den sicheren, verschlüsselten Tunnel zum VPN Head-End-Gerät aufbauen sowie Connection State Enforcement-Funktionalität und die detaillierte Filterung der durch sie initiierten Sessionen bieten. Einzelne PCs im dezentralen Netzwerk benötigen keine VPN Client-Software für den Zugriff auf Unternehmensressourcen. Da die Stateful-Firewall den Zugang zum Internet schützt, muss auf den einzelnen PCs nicht unbedingt eine individuelle Firewall-Software installiert werden. Der Netzwerkadministrator kann durch Implementierung individueller Firewall-Software auch auf den PCs am dezentralen Standort jedoch eine zusätzliche Sicherheit realisieren. Diese Konfiguration kann sinnvoll sein, wenn der Heimarbeiter auch mobil arbeitet und über das öffentliche Telefonnetz direkt auf das Internet zugreift. Da wir die Hosts durch eine Stateful-Firewall absichern, kann der dezentrale Standort direkt auf das Internet zugreifen, statt alle Zugriffe über die Zentrale durchzuführen. Außer wenn bei der Kommunikation mit der Zentrale NAT eingesetzt wird, sind die IP-Adressen der Geräte am dezentralen Standort so zu vergeben, dass sie sich nicht mit dem Adressraum in der Zentrale oder an einem anderen dezentralen Standort überschneiden. Geräte am dezentralen Standort, die einen direkten Internetzugang benötigen, erfordern eine Adressumsetzung auf eine registrierte Adresse. Diese Adressumsetzung kann realisiert werden, indem man alle in das Internet gerichteten Sessions in die öffentliche IP-Adresse der Firewall selbst übersetzt.

Zugang und Autorisierung für das Unternehmensnetzwerk und das Internet werden durch die Konfiguration sowohl der Firewall am dezentralen Standort und des VPN Head-End-Gerätes bestimmt. Konfigurieren und Sicherheitsmanagement der Firewall am dezentralen Standort können über einen IPSec Tunnel von der öffentlichen Seite der Firewall bis zur Unternehmenszentrale durchgeführt werden. Diese Anordnung stellt sicher, dass die Benutzer am dezentralen Standort keine Konfigurationsänderungen an der Firewall im Heimbüro vornehmen müssen. Die Authentifizierung sollte an der Firewall eingerichtet werden, so dass lokale Benutzer nicht versehentlich ihre Firewall-Konfiguration verändern und damit die Sicherheitspolicy für das betreffende Gerät in Frage stellen können. Die einzelnen Benutzer am dezentralen Standort, die auf das Unternehmensnetzwerk zugreifen, werden mit dieser Option nicht authentifiziert. Stattdessen verwenden die Firewall am dezentralen Standort und der VPN Head-End eine Geräte-Authentifizierung.

Um zu verhindern, dass Viren und Trojanische Pferde die einzelnen PCs am dezentralen Standort (ebenso wie jeden anderen PC im gesamten Unternehmen) befallen, wird weiterhin die Verwendung einer Virenscan-Software empfohlen.

Hardware VPN Client

Der Hardware VPN Client ist identisch mit der externen Firewall, verfügt aber nicht über eine residente Stateful-Firewall. Diese Konfiguration erfordert die Verwendung einer individuellen Firewall an den einzelnen Hosts, besonders wenn Split Tunnelling aktiviert ist. Ohne eine individuelle Firewall ist die Sicherheit der einzelnen Hosts nach dem VPN-Gerät davon abhängig, dass der Eindringling nicht in der Lage ist, die NAT (Network Address Translation) zu umgehen. Der Grund hierfür ist, dass bei Aktivierung des Split Tunnelling die Verbindungen ins Internet über eine einfache “many-to-one” NAT-Umsetzung erfolgen und keine Filterung in Layer 4 oder darüber durchlaufen. Bei deaktiviertem Split Tunnelling müssen alle Internetzugriffe über die Zentrale erfolgen. Diese Konfiguration macht individuelle Firewalls an den Endsystemen zumindest teilweise überflüssig.

Die Verwendung eines Hardware-Client bietet zwei wichtige Vorteile. Erstens werden wie beim Software VPN Client der Zugang und die Autorisation für das Unternehmensnetzwerk und das Internet zentral in der Unternehmenszentrale gesteuert. Konfigurieren und Sicherheitsmanagement des Hardware VPB Client selbst erfolgen über eine SSL-Verbindung von der Zentrale aus. Diese Anordnung stellt sicher, dass die Benutzer am dezentralen Standort keine Konfigurationsänderungen am Hardware VPN Client vornehmen müssen. Der zweite Vorteil des Hardware VPN Client besteht darin, dass die einzelnen PCs im Netzwerk am dezentralen Standort keine VPN Client-Software benötigen, um auf Ressourcen im Unternehmensnetzwerk zuzugreifen. Jedoch werden die einzelnen Benutzer, die vom dezentralen Standort aus auf das Unternehmensnetzwerk zugreifen, mit dieser Option nicht authentifiziert. Stattdessen authentifizieren sich der Hardware VPN Client und der VPN Head-End-Konzentrator gegenseitig.

Zugang über einen externen Router

Der Zugang über den externen Router ist nahezu identisch mit dem Zugang über eine externe Firewall, mit einigen Ausnahmen. Beim Einsatz nach einem Standalone-Breitband-Zugangsgerät besteht der einzige Unterschied darin, dass der Router weitergehende Applikationen wie QoS, Routing und mehr Verkapselungsmöglichkeiten unterstützt. Wenn die Breitbandfähigkeit in den Router integriert ist, wird kein eigenes Breitband-Zugangsgerät mehr benötigt. Diese Option setzt voraus, dass der ISP dem Anwender erlaubt, das Management des Breitband-Routers selbst zu übernehmen, was unüblich ist.

Schlussbemerkung

SAFE ist eine Richtlinie zur Implementierung von Sicherheit im Netzwerk. Das Konzept ist nicht als Sicherheitspolicy für Netzwerke gedacht, und auch nicht als allumfassendes Design zur Realisierung einer hundertprozentigen Sicherheit für alle bestehenden Netzwerke. SAFE ist vielmehr eine Vorlage, auf deren Grundlage die Netzwerkdesigner ihre Unternehmensnetzwerke gestalten und implementieren können, um die Sicherheitsanforderungen zu erfüllen.

Das Einrichten einer Sicherheitspolicy sollte immer der erste Schritt bei der Umwandlung des Netzwerks in eine sichere Infrastruktur sein. Nachdem diese Policy festgelegt worden ist, muss der Netzwerkdesigner die im ersten Teil dieses Dokumentes genannten Sicherheitsgrundsätze berücksichtigen und die Policy im Detail auf die bestehende Netzwerk-Infrastruktur abbilden.

Die SAFE-Architektur ist flexibel genug, um sich den meisten Netzwerken anzupassen. Mit SAFE können die Designer die Sicherheitsanforderungen aller Netzwerkfunktionen nahezu unabhängig voneinander erfüllen. Jedes Modul ist praktisch in sich abgeschlossen und geht von der Annahme aus, dass jedes damit verbundene Modul nur eine elementare Sicherheit bietet. Dies ermöglicht ein schrittweises Vorgehen zur Absicherung des gesamten Netzwerks. Anhand der Policy lassen sich somit die wichtigsten Netzwerkfunktionen schützen, ohne dass das Netzwerk von Grund auf neu konzipiert werden muss.

Klassifizierung der Architektur und Zeichenerklärung

Anwendungsserver: Stellt den Endbenutzern direkt oder indirekt Anwendungsdienste im Unternehmen zur Verfügung. Die Dienste umfassen unter anderem Workflow, allgemeine Bürotätigkeiten und Sicherheitsanwendungen.

Arbeitsstation oder Benutzerterminal: Eine Arbeitsstation oder ein Benutzerterminal ist ein Gerät im Netzwerk, das direkt von einem Endbenutzer verwendet wird. Dazu zählen unter anderem PCs, IP-Telefone und drahtlose Geräte.

Cisco IOS Firewall: Erweiterung der Cisco IOS Software um eine integrierte Firewall mit Stateful-Packet-Filterung.

Cisco IOS Router: Der Cisco IOS Router weist ein breites Spektrum an flexiblen Netzwerkgeräten auf, die zahlreiche Routing- und Sicherheitsdienste für alle Leistungsanforderungen zur Verfügung stellen. Die meisten Geräte sind modular und mit verschiedenen physikalischen LAN- und WAN-Schnittstellen ausgestattet.

Firewall (Stateful): Dieses Gerät zur Stateful-Packet-Filterung verwaltet Zustandstabellen für IP-basierte Protokolle. Datenverkehr kann die Firewall nur passieren, wenn er den definierten Zugangskontroll-Filtern entspricht oder wenn es sich um eine bereits initiierte Session in der Zustandstabelle handelt.

Host IDS: Host-basierte Intrusion Detection Systeme (HIDS) sind Software-Anwendungen, die Aktivitäten auf einem einzelnen Host überwachen. Zu den Überwachungstechniken zählen die Validierung von Betriebssystem- und Applikationsaufrufen, die Überprüfung von Protokoll-Dateien, Dateisysteminformationen und Netzwerkverbindungen.

Layer-2-Switch: Ein Layer-2-Switch bietet Bandbreite und VLAN-Dienste (Virtual LAN) für die Netzwerksegmente auf Ethernetebene. Die Geräte bieten in der Regel geswitchte 10/100-Ports, Gigabit Ethernet Uplinks, VLAN-Trunking und Funktionen zur Layer-2-Filterung.

Layer-3-Switch: Ein Layer-3-Switch bietet ähnlich hohe Übertragungsraten wie ein Layer-2-Switch mit zusätzlichen Routing-, QoS- und Sicherheitsfunktionen. Der Switch ist oft mit Prozessoren für spezielle Funktionen ausgestattet.

Managementserver: Der Managementserver bietet Dienste für das Netzwerk-Management für die Betreiber von Unternehmensnetzen. Diese Dienste umfassen unter anderem allgemeines Konfigurationsmanagement, Monitoring von Geräten für die Netzwerksicherheit und Ausführung von Sicherheitsfunktionen.

Network IDS: Netzwerk-basierte IDS (NIDS) werden üblicherweise non-disruptive eingesetzt. Dieses Gerät überwacht den Datenverkehr in einem LAN-Segment und versucht, Echtzeitdatenverkehr mit bekannten Angriffssignaturen zu vergleichen. Die Signaturen reichen von unteilbaren (ein einziges Paket in nur einer Richtung) bis zu zusammengesetzten Signaturen (mehrere Pakete), für die Zustandstabellen und Layer-7-Anwendungsüberwachung erforderlich sind.

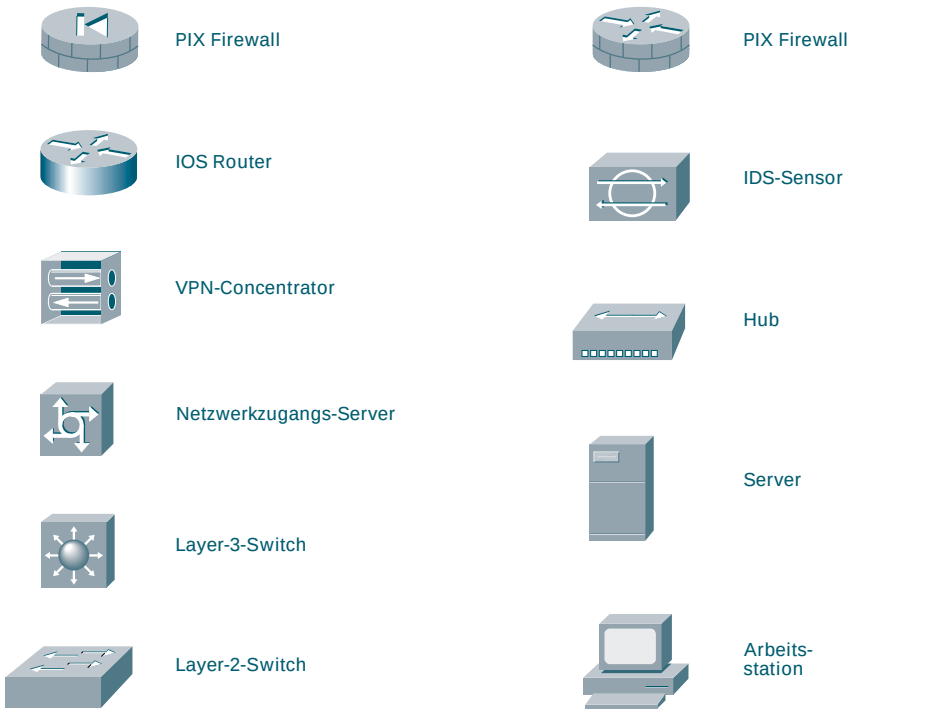
SMTP-Server zur Filterung von Inhalten: Die Anwendung wird in der Regel auf einem externen SMTP-Server ausgeführt, der die Inhalte und Anhänge von ein- und abgehenden E-Mails überwacht. Er entscheidet darüber, ob eine E-Mail unverändert weitergeleitet, verändert und weitergeleitet oder zurückgewiesen wird.

URL-Filterungsserver: Die Anwendung wird in der Regel auf einem Standalone-Server ausgeführt, der URL-Anforderungen, die von einem Netzwerkgerät weitergeleitet wurden, überwacht. Er setzt das Netzwerkgerät in Kenntnis, ob die Anfrage zum Internet weitergesendet wird.

Ein Unternehmen hat so die Möglichkeit, eine Sicherheits-Policy zu implementieren, durch die bestimmt wird, auf welche Internetseiten kein Zugriff erlaubt wird.

VPN-Terminierungsgerät: Dieses Gerät terminiert IPSec-Tunnel für VPN-Verbindungen (Site-to-Site oder Fernzugang). Es sollte zusätzliche Dienste bieten, damit dieselbe Netzwerkfunktionalität wie in einer klassischen WAN- oder Einwahlverbindung geboten wird.

Abbildung 15: Zeichenerklärung.



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134–1706
USA

Tel: +1 408 526 4000 800
553 NETS (6387)
Fax: +1 408 526 4100

European Headquarters
Cisco Systems Europe s.a.r.l.
11, Rue Camille Desmoulins
92782 Issy–les–Moulineaux
Cedex 9
France

Tel: +33 1 58 04 60 00
Fax: +33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134–1706
USA

Tel: +1 408 526–7660
Fax: +1 408 527–0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 9, 80 Pacific Highway
P.O. Box 469
North Sydney
NSW 2060 Australia

Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems hat mehr als 200 Niederlassungen in den folgenden Ländern. Adressen, Telefon- und Faxnummern entnehmen Sie bitte der Cisco.com-Website unter www.cisco.com/go/offices

Argentinien • Australien • Belgien • Brasilien • Chile • China • Costa Rica • Dänemark • Deutschland • Dubai (VAE) • Finnland • Frankreich • Großbritannien • Hongkong Indien • Indonesien • Irland • Israel • Italien • Japan • Kanada • Kolumbien • Korea • Kroatien • Luxemburg • Malaysia • Mexiko • Neuseeland • Niederlande Norwegen• Österreich • Peru • Philippinen • Polen • Portugal • Puerto Rico • Rumänien • Russland • Saudi-Arabien • Schweden • Schweiz • Singapur • Slowakei Slowenien • Spanien • Südafrika • Taiwan • Thailand • Tschechische Republik • Türkei • Ukraine • USA • Venezuela • Vietnam • Zimbabwe