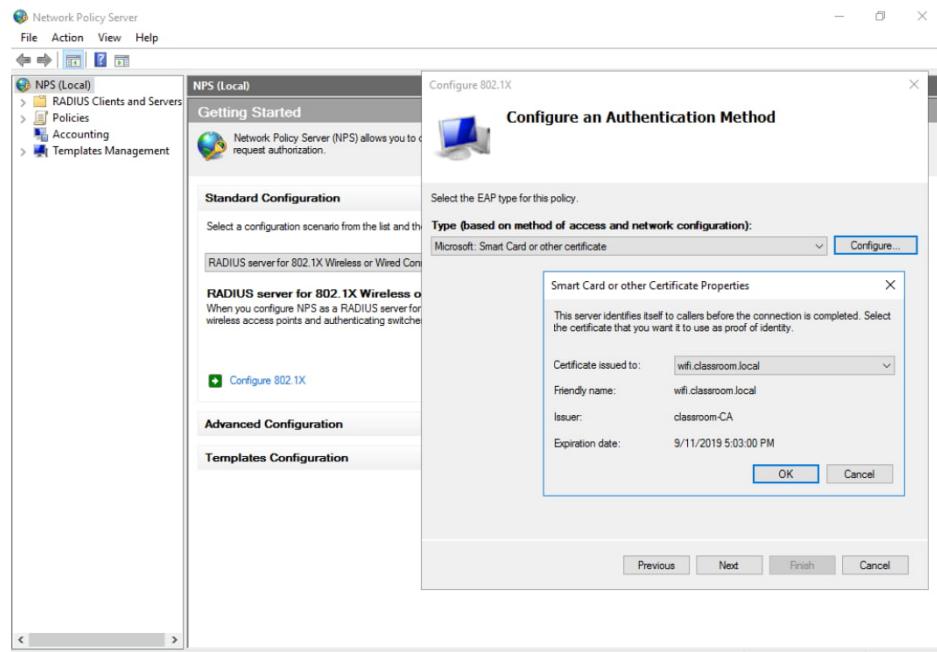


CiscoのVirtual Wireless LAN Controllerを用いて、WLANのセキュリティポリシーを設定する—このポリシーはWPA2の使用と、802.1X（エンタープライズ）認証の使用を強制します。
(スクリーンショットはCiscoからの許可を得て使用)

拡張認証プロトコル

拡張認証プロトコル(EAP)は、認証メカニズム自身の詳細でなく、認証メカニズムを取り決めるフレームワークを定義するものです。ベンダーはそのプロトコルに拡張を記述することで、サードパーティのセキュリティデバイスをサポートできます。EAPを実装するものとして、スマートカード、ワンタイムパスワード、生体認証、またはより単純なユーザー名とパスワードの組み合せがあります。

EAP-TLSは最も強力な認証タイプの1つであり、非常に広くサポートされています。認証サーバーとサブリカント上で公開鍵証明書を使用し、サブリカントと認証サーバーとの間で暗号化されたTLS (Transport Layer Security)トンネルが確立されます。サブリカントとサーバーのいずれも証明書で構成するので、これは相互認証を提供します。サブリカントは通常、スマートカードを用いて証明書を提供しますが、クライアントデバイスに証明書が、おそらくTPM (Trusted Platform Module)に、インストールされることもあります。



Network Policy Serverを構成して、802.1X EAP-TLSを用いるワイヤレスクライアントを認証する。
(スクリーンショットはMicrosoftからの許可を得て使用。)

PEAP、EAP-TTLS、およびEAP-FAST

各ワイヤレスデバイスに証明書を提供するのは、管理上の大きな課題です。サーバー側の証明書だけでセキュアなトンネルを提供する、その他のタイプのEAPが開発されています。

PEAP (Protected Extensible Authentication Protocol)

EAP-TLS同様、**PEAP (Protected Extensible Authentication Protocol)**においても、サブリカントと認証サーバーとの間で暗号化されたトンネルが確立されますが、PEAPではサーバーサイドの公開鍵証明書だけが求められます。サブリカントは証明書を必要としません。サーバーがサブリカントに認証されると、スニッフィング、パスワード推測/辞書攻撃、およびオンラインパス攻撃への保護を有するセキュアなトンネル経由で、ユーザー認証が行われます。このユーザー認証方式（「内部」方式とも呼ばれます）では、MS-CHAPv2またはEAP-GTCのいずれかが用いられます。Generic Token Card (GTC)方式は、ネットワークディレクトリに認証用トークンを送信するか、ワンタイムパスワードのメカニズムを使用するものです。

EAP-TTLS (EAP with Tunneled TLS)

EAP-TTLS (EAP-Tunneled TLS)は、PEAPと同様のものです。これはサーバーサイドの証明書を使用することで、ユーザーの認証情報が認証サーバーに送信される、保護されたトンネルを確立します。PEAPとの主な違いは、EAP-TTLSがあらゆる内部認証プロトコル（PAPまたはCHAPなど）を使用できる一方、PEAPではEAP-MSCHAPかEAP-GTCを使用しなければならないことです。

EAP-FAST (EAP with Flexible Authentication via Secure Tunneling)

EAP-FAST (EAP with Flexible Authentication via Secure Tunneling)もPEAPと同様のものですが、証明書を用いてトンネルを確立する代わりに、認証サーバーのマスターキーから各ユーザー向けに生成されるPAC (Protected Access Credential)を用いています。EAP-FASTにまつわる問題点として、アクセスを必要とする各ユーザーにPACを安全に配布する（提供する）ことが挙げられます。PACはアウトオブバンドの方法で、またはデジタル証明書を持つサーバーを介して配布することができます（ただし後者の場合、EAP-FASTはPEAPの使用に比べてさほど大きな利点をもたらしません）。あるいは、匿名のディフィー・ヘルマン鍵共有を介してPACを配布することもできます。ここで問題点として、アクセスポイントをユーザーに認証するものが何もない、ということがあります。不正アクセスポイントが十分な量のユーザー認証情報を取得し、ASLEAPパスワードクラッキング攻撃を行うこともあります(techrepublic.com/article/ultimate-wireless-security-guide-a-primer-on-cisco-eap-fast-authentication)。

RADIUSフェデレーション

ほとんどの場合、EAPを実装する際にはRADIUSサーバーが使用され、各ユーザー（サプリカント）ごとに認証情報の確認を行います。RADIUSフェデレーションは、複数の組織がそれぞれのRADIUSサーバーをRADIUS階層またはメッシュに結合することで、互いのユーザーへのアクセスを許可することを意味します。一例を挙げると、widget.fooのボブがgrommet.fooのネットワークにログオンする必要がある場合、grommet.fooのRADIUSサーバーは、ボブがローカルユーザーでない、そのリクエストをwidget.fooのRADIUSサーバーに転送することによりアクセス権を与えられていることを認識します。

RADIUSフェデレーションの一例としてeduroam network (eduroam.org)があり、異なる国の大学の学生が、「自国の」大学が保存している認証情報を使用して、すべての参加組織のネットワークにログオンできるようにしています。

不正アクセスポイントとエビルツイン

不正アクセスポイントは、悪意があるか否かにかかわらず、承認を受けずにネットワークにインストールされたアクセスポイントのことです。定期的にサイトを調査して不正なWAPを検出することが不可欠です。悪意のあるユーザーは、テザリング機能付きのスマートフォンといった基本的なものを用いてそうしたアクセスポイントをセットアップすることができ、悪意のないユーザーがそのようなアクセスポイントを偶然有効化してしまうかもしれません。セキュリティなしでLANに接続すると、不正なWAPがバックドアを生み出し、そこを通じてネットワークを攻撃します。また不正なWAPは、ユーザーのログオン試行を傍受し、中間者攻撃やプライベート情報へのアクセスを可能にするためにも使用されます。

正当なWAPを装う不正なWAPはエビルツインと呼ばれます。エビルツインは、正当なものと名前(SSID)が似ているだけかもしれませんし、脅威アクターが何らかのDoS技術を使って正当なWAPの動作を妨害するかもしれません。WAP上で認証セキュリティが有効化されていれば、脅威アクターが認証方法の詳細を知らない限り、攻撃が成功することはできません。しかし、ユーザーが誤って入力した認証情報から、エビルツインが認証に関する情報を取得できる場合もあります。



Cambium Networks (旧称Xirrus) Wi-Fi Inspectorを使用してWi-Fiネットワークを調査する—オープン認証(セキュリティなし)で構成されたプリントデバイスと、スマートTVアプライアンス(認証が必要)の存在に注意してください。(スクリーンショットはXirrusからの許可を得て使用)

不正なハードウェアWAPは、物理的検査によって突き止めることができます。また、inSSIDer (metageek.com/products/inssider)、Kismet (kismetwireless.net)、およびCambium Networks (旧名Xirrus) Wi-Fi Inspector (cambiumnetworks.com/products/software/wifi-designer-and-wifi-inspector)など、不正なWAPを検出できるさまざまなWi-Fiアナライザや監視システムがあります。

認証解除攻撃、アソシエーション切断攻撃、リプレイ攻撃

不正なWAPの使用に、**認証解除**攻撃が組み合わされることもあります。これは偽装されたフレームのストリームを送信し、クライアントがWAPから認証解除するように仕向けます。認証解除(deauthentication)フレームは、標的ステーションのMACアドレスを偽装しています。これにより、脅威アクターはネットワーク鍵の回収を目的とするリプレイ攻撃を実行したり、不正なWAPを挟み込んだりすることが可能になります。

同様の攻撃として、そのステーションの認証を完全に解除するのではなく、アソシエーション切断(disassociation)フレームで標的を襲うものがあります。切断されたステーションは完全には切り離されませんが、再度接続しない限りそのネットワーク上で通信することができません。いずれの攻撃も、ワイヤレス基盤に対するサービス拒否攻撃を実行するために使用されます。そのワイヤレス基盤が管理フレームの保護(MFP: Management Frame Protection/802.11w)をサポートしていれば、攻撃は緩和されます。WAPとクライアントのいずれも、MFPをサポートするように構成しなければなりません。

事前共有鍵認証は、ワイヤレスステーションがアクセスポイントと連携する際に、そのパスフレーズのハッシュを傍受することを目的とした、さまざまなタイプのリプレイ攻撃に対して脆弱です。ひとたびハッシュが傍受されると、オフラインのブルートフォース攻撃や辞書攻撃の標的となり得ます。WEPにおいて、これらは初期化ベクトル(IV)攻撃と呼ばれています。同じ鍵で毎回異なるキーストリームを生成するようになっているメカニズムの欠陥を悪用するからです。リプレイ攻撃の一種に、アクセスポイントに大量のパケットを生成させるものがあり、通常はステーションの認証解除、暗号化されたARPパケットの傍受、およびその急速なリプレイによって行われ、WAPがIV値を短期間で繰り返し、ハッシュ部分を明かすようにします。

WPAとWPA2はIV攻撃に対して脆弱ではありませんが、深刻な脆弱性が2017年に発見されました(krackattacks.com)。KRACK攻撃は4ウェイハンドシェイクを標的とするリプレイメカニズムを使用します。認証メカニズムがパーソナルかエンタープライズであるかに関係なく、KRACKは効果的です。クライアントとアクセスポイントの両方を、そうした攻撃に対して完全にパッチを適用することが重要です。

ジャミング攻撃

ワイヤレスネットワークは、他の電波発信源からの干渉によって妨害されることがあります。多くの場合、それは意図的なものではありませんが、脅威アクターがアクセスポイントを故意にジャミングする可能性もあります。これは単にサービスを妨害するために、またはデータを盗み出そうとネットワークにエビルツインを仕掛けるために行われます。Wi-Fiジャミング攻撃は、より強力な信号を発するWAPをセットアップすることで実行されます。またWi-Fiジャミングデバイスは広く出回っていますが、多くの場合その使用は違法であり、販売が違法であることもあります。そうしたデバイスは非常に小型ですが、それでも脅威アクターはワイヤレスネットワークへ物理的に非常に近く必要があります。

ジャミング攻撃を打ち破る唯一の方法は、攻撃側の電波発信源の位置を特定して無効化するか、正当な機器からの信号を強力にすることです。家庭向けや小規模企業向けのWAPではしばしば設定不可能ですが、CiscoのAironetシリーズといったより高度なワイヤレスアクセスポイントは、設定可能な出力レベルのコントロールをサポートしています。干渉源はスペクトラムアナライザを用いて検出することができます。Wi-Fiアナライザと違い、スペクトラムアナライザは特殊な無線受信機を用いる必要があります（Wi-Fiアダプターが、Wi-Fi信号以外のすべての信号を除去します）。通常、それらは指向性アンテナを持つ手持ち式のユニットとして提供され、干渉源の正確な位置を特定できるようになっています。

レビュー アク ティビティ：

セキュアなワイヤレスインフラストラクチャ

次の質問にお答えください。

1. 次の記述は正しいですか、誤りですか？帯域選択は、ワイヤレスネットワークのセキュリティに関するすべての要素に重大な影響を及ぼします。
2. ネットワーク管理者が、「シン」型アクセスポイントを用いてワイヤレスネットワークを実装することを推奨しています。どのような追加のアプライアンスやソフトウェアが必要ですか？またそれにはどのようなセキュリティ上の利点がなければなりませんか？
3. 事前共有鍵とは何ですか？
4. WPSは企業ネットワークに適した認証方法ですか？
5. ドメイン発行のデジタル証明書を持つクライアントだけがネットワークに加わるというワイヤレスネットワークを、あなたはデプロイ（展開）しようとしています。どのような認証メカニズムが適していますか？
6. ジョンは仕事用のラップトップを与えられ、現在出張中です。ホテルに到着した彼がラップトップの電源をオンにしたところ、ホテルの名前が付いたワイヤレスアクセスポイントを見つけたので、仕事の連絡をしようとそこに接続しました。ジョンはどのワイヤレス脅威の被害者になる恐れがありますか？

トピック9D

ロードバランサーを実装する



対象試験範囲

- 1.4 与えられたシナリオに基づいて、ネットワーク攻撃に関連する可能性のあるインジケーターを分析することができる。
3.3 与えられたシナリオに基づいて、セキュアなネットワークデザインを実装することができる。

サービス拒否(DoS)攻撃が甚大な被害をもたらし、それを緩和するのが非常に困難な場合があります。あなたはネットワークセキュリティのプロフェッショナルとして、DoSと分散型DoS (DDoS) の各手法を比較対照し、これらの攻撃に対してネットワークの耐性を強化するロードバランシング技術を推奨・構成できるようになる必要があります。

分散型サービス拒否攻撃

Webサイトやゲートウェイに対するサービス拒否(Denial of Service : DoS)攻撃のほとんどは分散型DoS (DDoS)です。これは、攻撃が複数のホストから同時に行われることを意味します。通常、脅威アクターはコマンド&コントロールネットワーク内でハンドラとして使用するために、マシンを侵害します。それらのハンドラは、DoSツール（ボット）によって数百、数千、あるいは数百万のホストを侵害し、ボットネットを形成します。

DDoS攻撃の中には、圧倒的な数のボットを使って、ネットワーク帯域を消費し、正規のホストに帯域を使用させないことを目的としたものがあります。その他のDDoS攻撃はCPUのサイクルとメモリを消費し、ホストの処理リクエストに対するリソース枯渇を生じさせます。このため、正当なトラフィックの処理が遅れ、ホストシステムを完全にクラッシュさせる可能性があります。一例を挙げると、**SYNフラッド攻撃**は、TCPの3ウェイハンドシェイクの際にクライアントのACKパケットを保留することで機能します。通常はクライアントのIPアドレスが偽装されますが、これは、不正なIPやランダムなIPが入力され、サーバーのSYN/ACKパケットが誤った宛先に送信されることを意味します。サーバー、ルーター、ファイアウォールは、そのステートテーブルに記録された保留中の接続のキューを保持することができます。クライアントからACKパケットを受信していないときは、接続がタイムアウトする前にSYN/ACK/パケットを一定回数再送信します。ここでの問題は、サーバーが限られた数の保留中の接続しか管理できず、DoS攻撃がそれをすぐに使い果たしてしまうことです。このことは、サーバーが正当なトラフィックに応答できないことを意味します。

アンプ攻撃、アプリケーション攻撃、およびOT攻撃

分散反射型DoS (DRDoS)攻撃、またはアンプSYNフラッド攻撃において、脅威アクターは被害者のIPアドレスになりますし、複数のサーバーで接続を開こうと試みます。それらのサーバーは、SYN/ACKレスポンスを被害者のサーバーに送信します。これにより、被害者が利用可能な帯域幅がすぐに消費されます。

アプリケーション攻撃

ネットワーク攻撃がSYNまたはSYN/ACKフラッディングなど低レベルの技術を使用しているのにに対し、アプリケーション攻撃は特定のアプリケーションプロトコルのヘッダーやペイロードにおける脆弱性を標的にしています。例えば、不正なクエリでDNSサービスを攻撃するタイプの**アンプ攻撃**があります。この技術の利点の1つに、リクエストが小さい一方、DNSクエリへのレスポンスに多数の情報を含めることができるので、脅威アクターのボットネット上の非常に限られたリソースで被害者のネットワークの帯域幅を圧倒できるという、非常に効果的な攻撃手段である、というものがあります。

NTP (Network Time Protocol)も同様のやり方で悪用できます。NTPは、ネットワークやインターネット上のサーバーが正確な時刻を維持するのをサポートします。多くのプロトコルやセキュリティメカニズムでは、サーバーとクライアントが同期していることが不可欠です。1つのNTPクエリー (monlist)を使って、NTPサーバーがコンタクトした直近の600台のマシンのリストを含むレスポンスを生成することができます。DNSアンプ攻撃と同じく小さいリクエストで、被害者のネットワークに大きなレスポンスを送信することができます。

OT (Operational Technology)攻撃

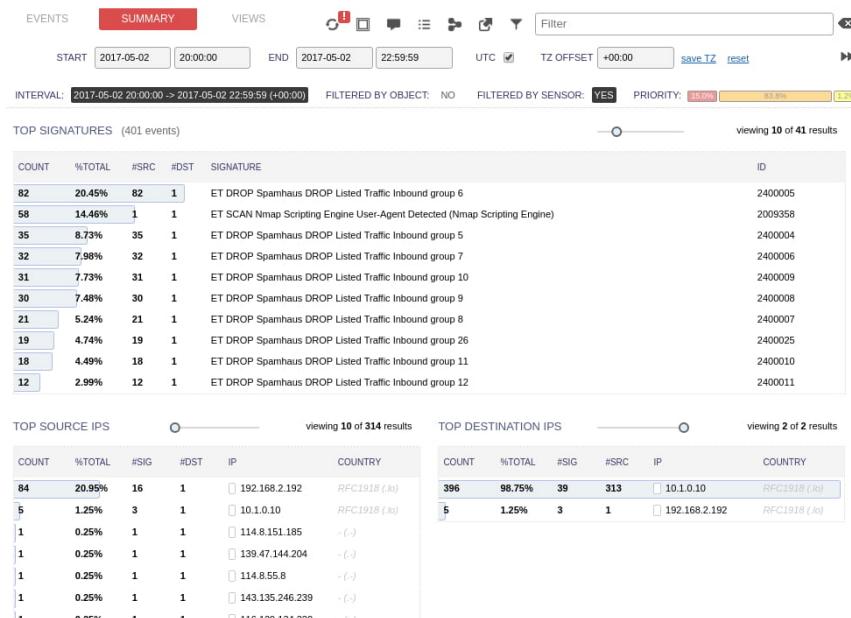
OT (Operational Technology)ネットワークは、組み込みシステムのデバイスとそのコントローラとの間で確立されます。「Operational」という用語が用いられているのは、それらのシステムがバルブ、モーター、電気スイッチ、ゲージ、センサーなど、物理的な電気機械部品の監視とコントロールを行っているからです。こうしたネットワーク内のコントローラに対するDDoS攻撃では、コンピューターネットワークに対する攻撃と同じ技術が用いられます。また、コントローラの中には処理能力が限られているタイプもあるので、Smurf (cloudflare.com/learning/ddos/smurf-ddos-attack)やPing of Death (impererva.com/learn/application-security/ping-of-death)といった古いタイプのDDoSテクニックが、組み込みシステムに対して引き続き効果的である場合もあります。こうしたデバイスのリソースが限られていることは、利用可能なメモリやCPU時間がDDoSによってすぐに消費されることを意味します。



組み込みシステムは攻撃のターゲットとなるだけでなく、ボットとして使用されることもあります。すべてのタイプのインターネット対応デバイスは、侵害に対して脆弱です。これにはWeb対応のカメラ、SOHOルーター、スマートTV、およびその他のアプライアンスが含まれます。これはInternet of Things (IoT)ボットネットと呼ばれます。

分散型サービス拒否攻撃の軽減

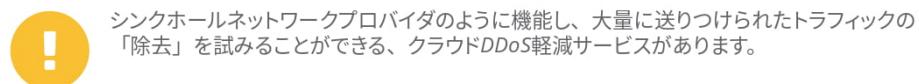
DDoS攻撃は正当な理由がないトラフィックの急増によって診断できますが、通常はロードバランシングやクラスターサービスなど、可用性の高いサービスを提供することでしか対抗できません。ステートフルファイアウォールがDDoS攻撃を検知し、自動的に発信元をブロックできる場合もあります。しかし、DDoS攻撃で用いられるテクニックの多くでは、発信元アドレスがランダムに偽装されるか、ボットによって発信されることになるので、攻撃源の検知は困難です。



Security Onion IDSを使用して、ブラックリストに入れられたIP範囲からのトラフィックをドロップする。
(スクリーンショットはSecurity Onionから許可を得て使用)

ネットワークがDDoS攻撃や同種のフラッディング攻撃に直面した際、ISPはアクセス制御リスト(ACL)またはブラックホールを用いることで、影響を受けたIPアドレスへのパケットをドロップすることができます。ブラックホールは、そのネットワークの他の部分が到達できないネットワークの領域です。数ギガバイトに上るストリームの各パケットをACLに照らして評価すると、処理リソースが消費されてしまうので、ブラックホールの方が好まれています。BGP (Border Gateway Protocol)ルーティングでこれを実行する標準的な方法は、**RTBH (Remotely Triggered Blackhole)** (cisco.com/c/dam/en_us/about/security/intelligence/blackhole.pdf)と呼ばれています。またブラックホールは、ISPのその他のカスタマーに対するダメージも軽減します。いずれのアプローチでも、正当なトラフィックはDDoSパケットと共に破棄されます。

別の選択肢として**シンクホールルーティング**を使用し、ある特定のIPアドレスに大量に送りつけられるトラフィックを、分析可能な別のネットワークに転送するというものがあります。一部の正当なトラフィックが通過を許可されることがありますが、真の利点は攻撃源を突き止め、それをフィルターする規則を設定できることです。次いでターゲットは短いTTLのDNSレコードを使って、そのサービス用のIPアドレスを変更し、正当なトラフィックが大量に送りつけられたデータを通過できるよう試みることができます。

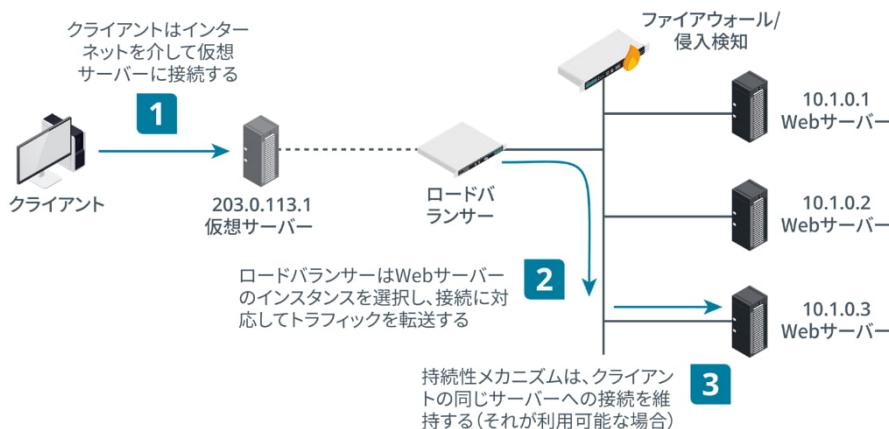


ロードバランシング

ロードバランサーは、ファームまたはプール内の利用可能なサーバーノードにリクエストを分配するものです。これは低負荷から高負荷まで対応できるサービスを提供するため、またDDoS攻撃を軽減するために用いられます。ロードバランサーは耐障害性ももたらします。あるファーム内で複数のサーバーが利用可能で、そのすべてのサーバーがロードバランサーを介して単一の名前/IPアドレスがアクセスされる場合、1つのサーバーが故障したとしても、クライアントのリクエストはファーム内の別のサーバーへ転送することができます。同じ機能を提供する複数のサーバーがある状況なら、いつでもロードバランサーを使用できます。その例として、Webサーバー、フロントエンド電子メールサーバー、Web会議、オーディオ/ビデオ会議、およびメディアストリーミングサーバーがあります。

ロードバランサーには、主に次の2種類があります。

- 第4層ロードバランサー — 基本的なロードバランサーで、IPアドレスとTCP/UDPポート値を基に転送の決定を行い、OSIモデルのトランスポート層で機能します。
- 第7層ロードバランサー (コンテンツスイッチ) — Webアプリケーションがますます複雑になっていることもあり、現在のロードバランサーは特定のURLへのリクエスト、またはビデオやオーディオのストリーミングといったデータタイプなど、アプリケーションレベルのデータを基に転送の決定を行える必要があります。これはより複雑なロジックを必要としますが、現在のアプライアンスの処理能力は、これに対処するのに十分です。



基本的なロードバランサーアーキテクチャのトポロジー。(画像提供: © 123RF.com)

スケジューリング

スケジュールアルゴリズムは、到着する各リクエストを処理するにあたり、どのノードを選択するかを決定するコードと基準です。最も単純なタイプのスケジューリングはラウンドロビンと呼ばれ、単に次のノードを選ぶことを意味します。別の手法として、接続が最も少ないノード、または応答時間が最も短いノードを選ぶということがあります。またそれぞれの手法は、管理者が設定した優先順位、または動的な負荷情報、もしくはその両方を使って加重化することができます。

さらにロードバランサーは、何らかのタイプのハートビートプローブ、またはヘルスチェックプローブを使用して、各ノードが利用可能かどうかや、負荷がかかっているかどうかを確認しなければなりません。第4層ロードバランサーが基本的な接続性テストしか行えない一方、第7層アプライアンスはホストの可用性だけを確認するのではなく、アプリケーションの状態をテストすることができます。

ソースIPアフィニティとセッションパーシステンス

クライアントデバイスがサーバーファーム内の特定のノードでセッションを確立すると、セッションが持続している間、その接続を使用し続けなければならないことがあります。ソースIPなしセッションアフィニティ(親和性)は、ユーザーセッションの扱いに関する第4層のアプローチです。これは、クライアントがセッションを確立すると、最初にそのリクエストを受け入れたノードに継続的に接続されることを意味します。

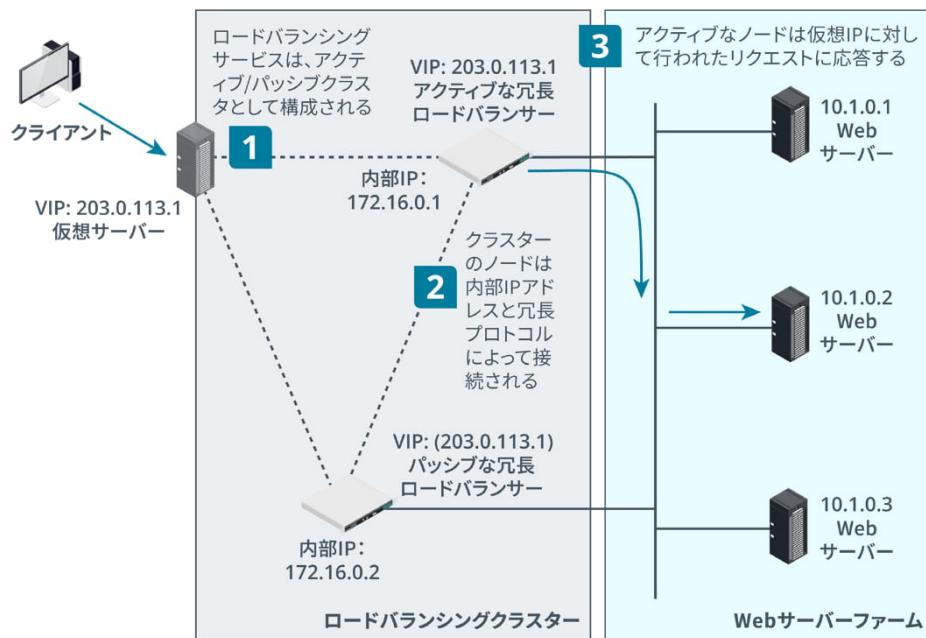
アプリケーション層のロードバランサーはパーシステンス(持続性)を用いることで、クライアントをセッションに接続したままにすることができます。通常、パーシステンスはノード上のCookie、またはロードバランサーによって挿入されたCookieを設定することで機能します。これはソースIPアフィニティよりも信頼できますが、ブラウザがCookieを受け入れる必要があります。

クラスタリング

ロードバランスが独立した処理ノードの間でトラフィックを分配する一方、クラスタリングは互いにデータを共有する複数の冗長処理ノードが接続を受け入れられるようにするものです。これは冗長性をもたらします。クラスタ内のノードの1つが停止すると、接続は機能しているノードにフェイルオーバーすることができます。クライアントにとって、そのクラスタは単一のサーバーに見えます。

仮想IP

例えば、片方が故障してももう1つがクライアントの接続を処理できるよう、2つのロードバランサー・アプライアンスをセットアップすることができます。単一のアプライアンスを用いたロードバランシングと違い、そのサービスへのアクセスに用いられるパブリックIPは、クラスタ内の2つのインスタンス間で共有されます。これは仮想IP、または共有（フローティング）アドレスと呼ばれます。各インスタンスはプライベート接続と共に構成され、それぞれが「現実の」IPアドレスで識別されます。この接続はCommon Address Redundancy Protocol (CARP)などの冗長プロトコルを実行し、アクティブなノードが仮想IPを「所有」して接続に応答できるようにします。また冗長性プロトコルはハートビートメカニズムを実装しており、アクティブなノードに障害が発生した場合に、パッシブノードへフェイルオーバーできるようにしています。



クラスタ化されたロードバランサーネットワークのトポロジー。(画像提供: © 123RF.com)

アクティブ/パッシブ(A/P)クラスタリングとアクティブ/アクティブ(A/A)クラスタリング

前節の例では、あるノードがアクティブである場合、もう1つのノードはパッシブでした。これは、アクティブ/パッシブクラスタリングと呼ばれます。アクティブ/パッシブ構成の主な利点に、フェイルオーバーの際もパフォーマンスが悪影響を受けないということがあります。しかし、未使用的処理能力のために、ハードウェアとオペレーティングシステムのコストが高くなります。

アクティブ/アクティブクラスターは、両方のノードが同時に接続を処理していることを意味します。これにより、すべてのノードが機能している間、管理者は利用可能なハードウェアから最大の処理能力を使用することができます。フェイルオーバーが発生した場合、故障したノードの負荷は直ちにしかも（ユーザーが気づかれないように）透過的に、残りのノードへ移動します。このとき、残りのノード上の負荷が高くなり、パフォーマンスが低下します。



標準的なアクティブ/パッシブ構成においては、アクティブノードの1つ1つがパッシブノードと対応していくなければなりません。アクティブノードよりも少ないパッシブノードをプロビジョニングしてコストを削減する、 $N+1$ および $N+M$ 構成があります。

アプリケーションクラスタリング

クラスタリングは、耐障害性の高いアプリケーションサービスを提供するためにも極めて一般的に使用されます。セッションの途中でアプリケーションサーバーに障害が発生すると、セッション状態データが失われます。アプリケーションクラスタリングにより、クラスタ内の各サーバーはセッション情報を互いに通信できるようになります。例えば、ユーザーがあるインスタンスにログインした場合、次のセッションは別のインスタンス上で開始され、新しいサーバーはログインの確立に用いられたCookieやその他の情報をアクセスできます。

Quality of Service (QoS : サービスの品質)

ほとんどのネットワークアプライアンスはベストエフォート方式と先入れ先出し(FIFO)方式でパケットを処理します。サービスの品質(QoS)は、トラフィックの特徴を基にその優先順位を決めるフレームワークです。これは主に、最小レベルの帯域幅を必要とし、レイテンシー（遅延）やジッター（ゆらぎ）の影響を受けやすい、音声および映像アプリケーションをサポートするのに用いられます。レイテンシー（遅延）は、送信されたデータが受信者に届くまでにかかる時間のことです。ミリ秒(ms)で測定されます。ジッター（ゆらぎ）は、その遅れの変動、またはパケット配達レートの一貫性がないこととして定義されています。FIFOベースのデリバリーは、同じネットワークを共有するその他のアプリケーションが帯域幅の喪失を引き起こし、リアルタイムサービスのレイテンシーとジッターを増加させる可能性を高めます。

さまざまな実行方法があり、数多くの異なるプロトコルやアプライアンスが関係するため、QoSの実装は複雑なプロジェクトになります。概して言えば、QoSは次のように実装されます。

- 組織はアプリケーションの検出を行い、使用中のプロトコルの帯域幅、遅延、ジッターのしきい値を特定し、それらの間の相対的な優先順位を決定します。次に、アプリケーションを第2層と第3層の標準的なCoS (Class of Service)コードにマッピングします。これらのコードは、QoSトラフィックを処理するホストと中間システムに設定されます。
- QoS対応のエンドポイントデバイスやアプリケーションは、IPヘッダー（第3層）内の**DiffServ**フィールドを使用し、イーサネットヘッダー（第2層）に802.1pフィールドを追加することで、そのパケットを優先順位の高いものとして扱わなければならないことを示します（トラフィックマーキング）。これはスイッチにフレームを送信します。
- そのスイッチがQoSをサポートしていれば、802.1pヘッダーを使用してそのフレームを優先させます。これは、外部へのトラフィックのキューを保持し、優先順位の低いフレームを遅らせることでのみ可能であることに注意してください。キューが満杯の場合、優先順位の低いフレームをドロップするかどうか、またはQoSの低下と引き換えにそのキューを消去すべきかどうかが、トラフィックポリシングポリシーに記述されていなければなりません。
- 同様のプロセスは、ネットワークの境界にあるルーターやロードバランサでも発生しますが、それらはDiffServ IPパケットヘッダーを検査することができ、より限定されている802.1pヘッダーに頼る必要はありません。優先順位の決定は常に外部向けのインターフェイス上で行われ、優先順位の低いトラフィックがキューの中に保持されていることに注意してください。



このプロセスには多くのバリエーションがあります。現在の第3層スイッチは、例えば802.1pタギングに依存するのではなく、DSCP値を検査することができます。QoSは、異なるタギングメカニズムを用いるワイヤレスネットワーク上でも実施が必要になるかもしれません。またIntServと呼ばれる、QoSに対する全く異なるアプローチも存在します。これはResource Reservation Protocol (RSVP)を用いることで、アプリケーションまたはポリシーによって要求されるパフォーマンス特性を有するリンクを取り決めるものです。

QoSマーキングは、DoS攻撃の可能性を生じさせます。脅威アクターが優先順位の高いものとして扱われるパケットを作り上げ、それらを高いレートで送信できると、ネットワークが動作停止に陥ります。QoSの一部として、トラフィックをマークするための正当な権限を確立するための信頼境界を設定することが含まれます。また、セキュリティ上重要な監視データや、ネットワークの管理/構成トラフィックのための十分な帯域幅を常に確保しなければなりません。



さらに詳しく学ぶには、Microsoft (docs.microsoft.com/en-us/skypeforbusiness/optimizing-your-network/expressroute-and-qos-in-skype-for-business-online) や Cisco (cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book/QoSIntro.html) が提供するケーススタディと設計の概要を活用してください。

レビュー アク ティビティ： ロードバランサー

次の質問にお答えください。

1. ネットワークDoS攻撃の多くが分散型なのはなぜですか？
2. アンプ攻撃とは何ですか？
3. ロードバランシングの状況でスケジューリングを行うとはどういう意味ですか？
4. ロードバランシングを使用している際、特定のサーバーノードにクライアントを連携させる方法のうち、最も信頼度の高いものを提供するのはどのメカニズムですか？
5. 次の記述は正しいですか、誤りですか？仮想IPは、2つのアプライアンスが障害に耐えるように構成され、同じIPアドレスへのリクエストに応答する手段である。
6. 第3層のQoSシステムにトラフィックマーキングを提供するのはどのフィールドですか？

レッスン9

概要

セキュアなネットワークアクセスのために、セグメント化ベースのネットワーク設計と設定、スイッチング、ルーティング、Wi-Fi、ロードバランシングの各テクノロジーを使用できる必要があります。

セキュアなネットワーク設計を実装するためのガイドライン

新規のネットワーク、または拡張されたネットワークの設計を実装する際は、次のガイドラインに従ってください。

- ビジネスワークフローと、それをサポートするサーバー、クライアント、プロトコルを特定します。設計を実装するためのVLAN、サブネット、ファイアウォールのポリシーを使用し、セキュリティ要件をサポートする、セグメント化されたネットワークゾーンまたはブロックを設計します。
- 次に挙げる特別な設計要件を満たすこととします。
 - インターネットに接続しているホスト向けの非武装地帯のトポロジー。
 - データセンター向けのイーストウェストおよびゼロトラスト設計。
 - IPv6アドレッシングのセキュアな実装。
- 各ブロックをサポートするスイッチングとルーティング機器とプロトコルを導入し、ループ保護、ポートセキュリティ、ルートセキュリティを確保します。
- Wi-Fiネットワークの適切な認証メカニズムを選択します。
 - EAPメソッド (EAP-TLS、EAP-TTLS、またはPEAP) を備えたエンタープライズ認証が最も優れたセキュリティをもたらします。
 - 事前共有鍵認証やパーソナル認証は、14文字以上のパスフレーズで構成する必要があります、互換性に関する問題がなければWPA3を使用すべきです。
 - リスクを理解しているという前提で、ゲストネットワーク向けにオープン認証を使用することもできます。
- サービス拒否攻撃で生じるリスクを評価し、ロードバランシングとクラスタ化が行われたサービスを設計し、高い可用性と耐障害性を実現します。
- ボイスオーバー IPや会議のサポートなど、サービスの品質(QoS)メカニズムに関する要件を評価します。

レッスン10

ネットワークセキュリティアプライアンスを実装する

レッスン概要

ネットワーク接続を実装するために用いられる、セキュアなスイッチングおよびルーティングのアプライアンスとプロトコルに加え、ネットワークインフラストラクチャの設計には、サービスとデータの機密性、完全性、可用性を保証するセキュリティアプライアンスも含めなければなりません。セキュリティおよび監視用のデバイスとソフトウェアの各機能の違いを理解し、それらのデバイスをネットワークのふさわしい場所にデプロイ（展開）できる必要があります。

レッスンの目的

このレッスンの内容は、以下のとおりです。

- ファイアウォールとプロキシサーバーを実装する。
- ネットワークセキュリティ監視を実装する。
- SIEMの使用を要約できる。

トピック10A

ファイアウォールとプロキシサーバーを実装する



対象試験範囲

3.3 与えられたシナリオに基づいて、セキュアなネットワークデザインを実装することができる。

ファイアウォールは最も長く使用されてきたネットワークセキュリティ管理であり、最初期のインターネットネットワークの一部を分離する目的で1980年代に開発されました。そうした初期の時代以来、ファイアウォールの種類と機能は拡大と深化を続けています。ネットワークセキュリティの専門家として、ファイアウォールとプロキシの実装、構成、そしてトラブルシューティングに勤務時間の大半を費やすことになるでしょう。

パケットフィルタリングファイアウォール

パケットフィルタリング型は最も初期のネットワークファイアウォールです。現在でもすべてのファイアウォールは、この基本機能を実行できます。

アクセス制御リスト(ACL)

パケットフィルタリングファイアウォールは、アクセス制御リスト(ACL)と呼ばれる一群のルールを規定することで構成されます。それぞれのルールは特定のタイプのデータパケットと、パケットがルールとマッチした際にとる適切な行動を定義しています。行動は、拒否（そのパケットをブロックまたはドロップし、場合によってはイベントをログに記録する）もしくは許可（そのパケットにファイアウォールを通過させる）のいずれかです。パケットフィルタリングファイアウォールはIP/パケットのヘッダーを検査できます。つまり、それらのヘッダーにある以下の情報に基づいてルールを作成できるのです。

- IPフィルタリング – 発信元IPアドレスや宛先IPアドレスを基準にトラフィックを許可または拒否します。
- プロトコルのID/タイプ (TCP、UDP、ICMP、ルーティングプロトコルなど)。
- ポートフィルタリング/セキュリティ – 発信元ポート番号や宛先ポート番号を基準にパケットを許可または拒否します (TCPまたはUDPアプリケーションの場合)。

一部の製品には、特定のタイプのICMP (ping) トラフィックだけを拒否する、あるいはハードウェア(MAC)アドレスによってフィルタリングするという、追加機能を備えたものもあります。別の区別として、そのファイアウォールがインバウンドトラフィックだけを制御できるか、またはインバウンドとアウトバウンドの両方のトラフィックを制御できるか、というものがあります。これはイングレス(ingress)トラフィック、イーグレス(egress)トラフィックまたはフィルタリングと呼ばれることもあります。許可されていないアプリケーションがネットワーク上で動作するのをブロックし、バックドアなどのマルウェアを撃退できるという点で、アウトバウンドトラフィックの制御は有益です。イングレスおよびイーグルストラフィックは、別々のACLを用いてフィルタリングされます。

ステートレスオペレーション

基本的なパケットフィルタリングファイアウォールは**ステートレス**です。これは、ネットワークセッションに関する情報を保存しないことを意味します。各パケットは独立して分析され、以前に処理されたパケットの記録はありません。このタイプのフィルタリングは最低限の処理しか必要と

しませんが、パケットのシーケンスに拡散する攻撃に対して脆弱である場合があります。また、何らかの種類のロードバランシングが使われている場合や、クライアントやサーバーが動的に割り当てられたポートを使用する場合のトラフィックフローに、ステートレスファイアウォールが問題を生じさせることもあります。

ステートフルインスペクションファイアウォール

ステートフルインスペクションファイアウォールは、2つのホスト間で確立されたセッションに関する情報をトラッキングすることで、または悪意ある試みによって不正なセッションが開始されるのをブロックすることで、これらの問題に対処します。現在の大半のファイアウォールには、何らかのレベルのステートフルインスペクション機能が組み込まれています。セッションデータはステートテーブルに保存されます。パケットが到着すると、ファイアウォールはそれをチェックし、既存の接続に属するものかどうかを判断します。そうでない場合、ファイアウォールは通常のパケットフィルタリングルールを適用して、それを許可するかどうかを決定します。通常、ひとたび接続が許可されると、ファイアウォールは処理負担を減らすため、監視せずにトラフィックを通過させます。

The screenshot shows the pfSense Diagnostic States page. At the top, there are tabs for 'States' (which is selected) and 'Reset States'. Below that is a 'State Filter' section with a dropdown for 'Interface' set to 'WAN' and a 'Filter expression' input field containing 'Simple filter such as 192.168, v6, icmp or ESTABLISHED'. A 'Filter' button is also present. The main area displays a table titled 'States' with columns: Interface, Protocol, Source (Original Source) -> Destination (Original Destination), State, Packets, and Bytes. The table lists several network connections:

Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes
WAN	icmp	172.16.0.254:10348 -> 172.16.0.253:10348	0:0	2.223 K / 2.223 K	61 KIB / 61 KIB
WAN	tcp	192.168.1.100:49423 -> 10.1.0.10:80 (172.16.0.254:80)	TIME_WAIT:TIME_WAIT	13 / 15	2 KIB / 14 KIB
WAN	tcp	192.168.1.100:49424 -> 10.1.0.10:80 (172.16.0.254:80)	TIME_WAIT:TIME_WAIT	46 / 92	3 KIB / 123 KIB
WAN	tcp	192.168.1.100:49425 -> 10.1.0.10:80 (172.16.0.254:80)	TIME_WAIT:TIME_WAIT	18 / 26	2 KIB / 31 KIB
WAN	tcp	192.168.2.192:32830 -> 10.1.0.10:80 (172.16.0.254:80)	TIME_WAIT:TIME_WAIT	8 / 7	802 B / 5 KIB
WAN	tcp	192.168.2.192:32832 -> 10.1.0.10:80 (172.16.0.254:80)	ESTABLISHED:ESTABLISHED	13 / 12	2 KIB / 10 KIB
WAN	tcp	192.168.1.100:49427 -> 10.1.0.10:80 (172.16.0.254:80)	ESTABLISHED:ESTABLISHED	11 / 20	1 KIB / 26 KIB

pfSenseファイアウォールアプライアンスのステートテーブル。(スクリーンショットはRubicon Communications, LLC.からの許可を得て使用。)

ステートフルインスペクションは、トランスポートとアプリケーションの2つのレイヤーで行われます。

トランスポートレイヤー（OSI第4層）

トランスポートレイヤーにおいて、ファイアウォールはTCP 3ウェイハンドシェイクを調べることで、新規の接続と確立済みの接続を区別します。正当なTCP接続は、SYN > SYN/ACK > ACKの順序でセッションを確立する必要があり、そのセッションはシーケンス番号を使ってトラッキングされます。ACKのないSYNやシーケンス番号の異常などのように、そこからの逸脱がある場合は、悪意のあるフラッディングまたはセッションハイジャックの試みとしてドロップされます。発信元IPアドレスをブロックし、セッションを絞ることでそうした攻撃に対処するよう、ファイアウォールを構成することもできます。UDP接続をトラッキングすることもできますが、UDPはコネクションレス型のプロトコルなので、難易度が高くなります。また、IPヘッダーとICMPの異常を検知できる可能性もあります。

Advanced Options	
Source OS	<input type="text" value="Any"/> <input checked="" type="checkbox"/>
Note: this only works for TCP rules. General OS choice matches all subtypes.	
Diffserv Code Point	<input type="text"/> <input checked="" type="checkbox"/>
Allow IP options	<input type="checkbox"/> Allow packets with IP options to pass. Otherwise they are blocked by default. This is usually only seen with multicast traffic.
Disable reply-to	<input type="checkbox"/> Disable auto generated reply-to for this rule.
Tag	<input type="text"/>
A packet matching this rule can be marked and this mark used to match on other NAT/filter rules. It is called Policy filtering.	
Tagged	<input type="text"/>
A packet can be matched on a mark placed before on another rule.	
Max. states	<input type="text"/>
Maximum state entries this rule can create.	
Max. src nodes	<input type="text"/>
Maximum number of unique source hosts.	
Max. connections	<input type="text"/>
Maximum number of established connections per host (TCP only).	
Max. src. states	<input type="text"/>
Maximum state entries per host.	
Max. src. conn. Rate	<input type="text"/>
Maximum new connections per host (TCP only).	
Max. src. conn. Rates	<input type="text"/>
/ per how many second(s) (TCP only)	
State timeout	<input type="text"/>
State Timeout in seconds (TCP only)	

*pfSense*ファイアウォールのルール構成 – 高度な設定により、状態と接続の最大数を設定することができます。(スクリーンショットはpfsense.orgからの許可を得て使用。)

アプリケーションレイヤー（OSI第7層）

アプリケーション対応のファイアウォールは、アプリケーションレイヤーでパケットの中身を検査することができます。主要な機能の1つに、アプリケーションプロトコルがポートとマッチしていることを検証するというものがあります。一例を挙げると、単にポート80が開いているという理由で、マルウェアがポート80を介して生のTCPデータを送信していないことを検証します。別の例として、WebアプリケーションファイアウォールはHTTPヘッダーと、HTTPパケット内にあるHTMLコードを分析し、脅威データベースにあるパターンとマッチするコードの特定を試みます。アプリケーション対応のファイアウォールには、アプリケーションレイヤーゲートウェイ、ステートフルマルチレイヤーインスペクション、あるいはディープパケットインスペクションなど、多くの異なる名称があります。アプリケーション対応のデバイスは、各タイプのトラフィック（HTTPおよびHTTPS、SMTP/POP/IMAP、FTPなど）に対応する個別のフィルターで構成しなければなりません。**アプリケーション対応のファイアウォール**は非常に強力ですが、脆弱性がないわけではありません。非常に複雑なために、ファイアウォールファームウェア内の悪用可能な脆弱性に対してDoS攻撃を仕掛けることができます。またSSL/TLSインスペクターと共に構成しない限り、ファイアウォールは暗号化されたデータパケットを検査できません。

iptables

`iptables`は多数のLinuxディストリビューションが提供しているコマンドラインユーティリティで、Linux kernelファイアウォールによって実行されるルールを管理者が編集できるようにしています(linux.die.net/man/8/iptables)。`iptables`はチェーンと共に動作し、ローカルホストを宛先とするトラフィック用のINPUTチェーンなど、さまざまなタイプのトラフィックに適用されます。それぞれのチェーンにはデフォルトポリシーが設定されており、ルールとマッチしないトラフィックをDROP(ドロップ)またはALLOW(許可)します。1つ1つのルールは順番に処理され、基準にマッチするトラフィックを許可するかドロップするかを決定します。